

DATA ENCRYPTION METHOD, DATA DECRYPTION METHOD, AND RELATED APPARATUSES

TECHNICAL FIELD

[0001] The present invention relates to the computer field, and in particular, to a data
5 encryption method, a data decryption method, and related apparatuses.

BACKGROUND

[0002] Currently, a common packet data encryption method is to divide to-be-encrypted
plaintext data into multiple plaintext data blocks that have exactly the same data length; and
for each plaintext data block, sequentially generate a corresponding ciphertext data block
10 based on a same encryption algorithm and by using a corresponding key, where data formed
by combining multiple generated ciphertext data blocks in sequence is ciphertext data that is
obtained after the to-be-encrypted plaintext data is encrypted.

[0003] A data encryption method based on an AES (Advanced Encryption Standard,
advanced encryption standard) algorithm is used as an example. A data processing length of
15 the AES algorithm is 128 bits, and therefore, in the data encryption method based on the AES
algorithm, to-be-encrypted plaintext data may be divided into multiple plaintext data blocks
with a data length of 128 bits, and if a length of the last plaintext data block obtained is less
than 128 bits, padding processing may be performed; for each plaintext data block, a
corresponding ciphertext data block is sequentially generated based on a same AES algorithm
20 and by using a corresponding key; and further, ciphertext data is obtained after the
to-be-encrypted plaintext data is encrypted.

[0004] However, usually, a data encryption speed is closely related to security strength of
an encryption algorithm. Selecting an encryption algorithm with higher security strength may

cause a lower data processing speed during data encryption, which cannot meet an application scenario requirement in most cases.

SUMMARY

[0005] Embodiments of the present invention provide a data encryption method, a data decryption method, and related apparatuses, so as to solve the problem of a relatively low data processing speed.

[0006] According to a first aspect, a data encryption method is provided, including:
dividing, based on a preset dividing manner, to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the same data length;

for each plaintext data block, sequentially determining that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext data block falls; and generating, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, where a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval; and

combining multiple generated ciphertext data blocks according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted.

[0007] With reference to the first aspect, in a first possible implementation manner, the preset length interval specifically includes two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0008] With reference to the first aspect, in a second possible implementation manner, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset initial key; and

when the plaintext data block is not the first plaintext data block among the

multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.

5 **[0009]** With reference to the first aspect, the first possible implementation manner of the first aspect, or the second possible implementation manner of the first aspect, in a third possible implementation manner, the generating, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block specifically
10 includes:

when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, performing an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypting the
15 operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, dividing the
20 plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially performing an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by
25 using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combining multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

30 **[0010]** With reference to the third possible implementation manner of the first aspect, in a

fourth possible implementation manner, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

[0011] With reference to the third possible implementation manner of the first aspect, in a fifth possible implementation manner, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

[0012] With reference to the third possible implementation manner of the first aspect, in a sixth possible implementation manner, the key corresponding to the plaintext data block is generated specifically in the following manner:

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and

a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

5 if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to
10 the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

[0013] With reference to the fourth possible implementation manner of the first aspect, or
15 the sixth possible implementation manner of the first aspect, in a seventh possible implementation manner, the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

20 **[0014]** According to a second aspect, a data decryption method is provided, including:
dividing, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length;

for each ciphertext data block, sequentially determining that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding
25 to a preset length interval within which a data length of the ciphertext data block falls; and generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, where a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption
30 algorithm corresponding to the preset length interval; and

combining multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted.

[0015] With reference to the second aspect, in a first possible implementation manner, the preset length interval specifically includes two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0016] With reference to the second aspect, in a second possible implementation manner, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

[0017] With reference to the second aspect, the first possible implementation manner of the second aspect, or the second possible implementation manner of the second aspect, in a third possible implementation manner, the generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block specifically includes:

when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypting the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and performing an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data

processing length of the decryption algorithm corresponding to the ciphertext data block, dividing the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypting the sub ciphertext data block based on the decryption algorithm
5 corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and performing an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combining multiple obtained sub plaintext data blocks according to a sequence of the multiple
10 sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

[0018] With reference to the third possible implementation manner of the second aspect, in a fourth possible implementation manner, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data
15 corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data
20 corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous
25 ciphertext data block.

[0019] With reference to the third possible implementation manner of the second aspect, in a fifth possible implementation manner, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational
30 data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

5 **[0020]** With reference to the third possible implementation manner of the second aspect, in a sixth possible implementation manner, the key corresponding to the ciphertext data block is generated specifically in the following manner:

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the
10 ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, performing an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the decryption algorithm
15 corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the
20 previous ciphertext data block, performing an exclusive-or operation on a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext
25 data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block.

[0021] With reference to the fourth possible implementation manner of the second aspect, or the sixth possible implementation manner of the second aspect, in a seventh possible implementation manner, the specified sub plaintext data block among the multiple sub
30 plaintext data blocks is specifically the first sub plaintext data block among the multiple sub

plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

[0022] According to a third aspect, a data encryption apparatus is provided, including:

a first dividing unit, configured to divide, based on a preset dividing manner,
5 to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the same data length;

an encrypting unit, configured to sequentially determine, for each plaintext data block, that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext
10 data block falls; and generate, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, where a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval; and

15 a first combining unit, configured to combine multiple generated ciphertext data blocks according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted.

[0023] With reference to the third aspect, in a first possible implementation manner, the
20 preset length interval specifically includes two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0024] With reference to the third aspect, in a second possible implementation manner, when the plaintext data block is the first plaintext data block among the multiple plaintext
25 data blocks, the key corresponding to the plaintext data block is a preset initial key; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext
30 data block, and by using a key corresponding to the previous plaintext data block.

[0025] With reference to the third aspect, the first possible implementation manner of the third aspect, or the second possible implementation manner of the third aspect, in a third possible implementation manner, the encrypting unit is specifically configured to: when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, perform an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially perform an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combine multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

[0026] With reference to the third possible implementation manner of the third aspect, in a fourth possible implementation manner, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data

corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

[0027] With reference to the third possible implementation manner of the third aspect, in a fifth possible implementation manner, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

[0028] With reference to the third possible implementation manner of the third aspect, in a sixth possible implementation manner, the encrypting unit is specifically configured to: when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data

blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key
5 corresponding to the plaintext data block.

[0029] With reference to the fourth possible implementation manner of the third aspect, or the sixth possible implementation manner of the third aspect, in a seventh possible implementation manner, the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub
10 plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

[0030] According to a fourth aspect, a data decryption apparatus is provided, including:
a second dividing unit, configured to divide, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly
15 the same data length;

a decrypting unit, configured to sequentially determine, for each ciphertext data block, that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generate, based on the decryption algorithm corresponding to
20 the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, where a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm corresponding to the preset length interval; and

a second combining unit, configured to combine multiple decrypted plaintext data
25 blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted.

[0031] With reference to the fourth aspect, in a first possible implementation manner, the preset length interval specifically includes two intervals: one preset length interval is a length
30 interval less than or equal to a specified length, and the other preset length interval is a length

interval greater than the specified length.

[0032] With reference to the fourth aspect, in a second possible implementation manner, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

[0033] With reference to the fourth aspect, the first possible implementation manner of the fourth aspect, or the second possible implementation manner of the fourth aspect, in a third possible implementation manner, the decrypting unit is specifically configured to: when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypt the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and perform an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypt the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and perform an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combine

multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

[0034] With reference to the third possible implementation manner of the fourth aspect, in a fourth possible implementation manner, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

[0035] With reference to the third possible implementation manner of the fourth aspect, in a fifth possible implementation manner, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

[0036] With reference to the third possible implementation manner of the fourth aspect, in a sixth possible implementation manner, the decrypting unit is specifically configured to: when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext

data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block.

[0037] With reference to the fourth possible implementation manner of the fourth aspect, or the sixth possible implementation manner of the fourth aspect, in a seventh possible implementation manner, the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

[0038] According to the data encryption method provided in the first aspect, the data decryption method provided in the second aspect, the data encryption apparatus provided in the third aspect, and the data decryption apparatus provided in the fourth aspect, to-be-encrypted plaintext data is divided into multiple plaintext data blocks that do not have exactly the same data length; and an encryption algorithm with higher security strength is used for a plaintext data block whose data length is relatively short, and an encryption algorithm with lower security strength is used for a plaintext data block whose data length is relatively long. This takes security into account, and in addition, data encryption duration

can be reduced and an overall data processing speed can be improved by using an encryption algorithm with lower security strength for a plaintext data block with a relatively long data length.

BRIEF DESCRIPTION OF DRAWINGS

5 [0039] Accompanying drawings are provided for further understanding of the present invention, which are a part of the specification and are used to explain the present invention together with embodiments of the present invention, but are not intended to limit the present invention. In the accompanying drawings:

[0040] FIG. 1 is a flowchart of a data encryption method according to an embodiment of
10 the present invention;

[0041] FIG. 2 is a flowchart of a ciphertext data block generating method according to an embodiment of the present invention;

[0042] FIG. 3 is a schematic diagram of a plaintext data block dividing manner according to an embodiment of the present invention;

15 [0043] FIG. 4 is a schematic diagram of a ciphertext data block generating manner according to an embodiment of the present invention;

[0044] FIG. 5 is a schematic diagram of a ciphertext data block combining manner according to an embodiment of the present invention;

[0045] FIG. 6 is a flowchart of a data decryption method according to an embodiment of
20 the present invention;

[0046] FIG. 7 is a flowchart of a plaintext data block generating method according to an embodiment of the present invention;

[0047] FIG. 8 is a schematic diagram of a ciphertext data block dividing manner according to an embodiment of the present invention;

25 [0048] FIG. 9 is a schematic diagram of a plaintext data block generating manner according to an embodiment of the present invention;

[0049] FIG. 10 is a schematic diagram of a plaintext data block combining manner according to an embodiment of the present invention;

[0050] FIG. 11 is a schematic structural diagram of a data encryption apparatus according to an embodiment of the present invention; and

[0051] FIG. 12 is a schematic structural diagram of a data decryption apparatus according to an embodiment of the present invention.

5

DESCRIPTION OF EMBODIMENTS

[0052] In order to provide an implementation solution for improving a data processing speed, embodiments of the present invention provide a data encryption method, a data decryption method, and related apparatuses. The following describes exemplary embodiments of the present invention with reference to the accompanying drawings for the specification. It should be understood that the exemplary embodiments described herein are merely used to describe and explain the present invention but are not intended to limit the present invention. And in a non-conflict condition, the embodiments of the application and features in the embodiments can separately be mutually combined.

[0053] An embodiment of the present invention provides a data encryption method. As shown in FIG. 1, the method includes the following steps:

[0054] Step 101: Divide, based on a preset dividing manner, to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the same data length.

[0055] Step 102: For each plaintext data block, sequentially determine that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext data block falls; and generate, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, where a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval.

[0056] Step 103: Combine multiple generated ciphertext data blocks according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted.

[0057] Because a data processing length of an encryption algorithm is a fixed value, if a

length of a data segment is less than the data processing length of the encryption algorithm, a padding operation needs to be first performed on the data, so that the length reaches the data segment processing length of the encryption algorithm, and then subsequent processing can be performed based on the encryption algorithm, which is the prior art and is not described in detail herein again.

[0058] Therefore, preferably, when the based preset dividing manner in step 101 is set, a data processing length of the encryption algorithm may be considered, to make a data length of each plaintext data block that is obtained by means of the dividing be an integral multiple of a data processing length of the encryption algorithm corresponding to the plaintext data block as much as possible, thereby reducing padding operations during a data encryption process, and improving an encryption speed. In this case, a padding operation may need to be performed only on the last plaintext data block.

[0059] The preset length interval includes at least two intervals, there is no intersection between preset length intervals, and all the preset length intervals constitute an entire length interval.

[0060] In an embodiment of the present invention, the preset length interval may specifically include two intervals. One specified length is set, and the entire length interval is divided into two preset length intervals by using the specified length. One preset length interval is a length interval less than or equal to the specified length, and a corresponding encryption algorithm is a first encryption algorithm; and the other preset length interval is a length interval greater than the specified length, and a corresponding encryption algorithm is a second encryption algorithm. Security strength of the first encryption algorithm is not lower than security strength of the second encryption algorithm.

[0061] That is, in this case, when a data length of a plaintext data block is less than or equal to the specified length, an encryption algorithm corresponding to the plaintext data block is the first encryption algorithm; when a data length of a plaintext data block is greater than the specified length, an encryption algorithm corresponding to the plaintext data block is the second encryption algorithm.

[0062] In another embodiment of the present invention, the preset length interval may specifically include three intervals. Two specified lengths, that is, a first specified length and a

second specified length, are set, and the first specified length is less than the second specified length. The entire length interval is divided into three preset length intervals by using the two specified lengths. The first preset length interval is a length interval less than or equal to the first specified length, and a corresponding encryption algorithm is a first encryption algorithm;
5 the second preset length interval is a length interval greater than the first specified length and less than or equal to the second specified length, and a corresponding encryption algorithm is a second encryption algorithm; and the third preset length interval is a length interval greater than the second specified length, and a corresponding encryption algorithm is a third encryption algorithm. In addition, security strength of the first encryption algorithm is not
10 lower than security strength of the second encryption algorithm, and security strength of the second encryption algorithm is not lower than security strength of the third encryption algorithm.

[0063] In other embodiments of the present invention, the preset length interval may specifically include more than three intervals, which is not described in detail herein again.

15 **[0064]** Further, for a key used to generate a ciphertext data block in step 102, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset initial key; and when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, a key generating manner in the prior art may be used, and preferably, in the embodiment of the
20 present invention, the key corresponding to the plaintext data block may be generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.

[0065] Preferably, in step 102, after the encryption algorithm corresponding to the
25 plaintext data block is determined, the generating, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block may specifically be shown in FIG. 2 and include the following steps:

[0066] Step 201: Determine whether the data length of the plaintext data block is less than
30 or equal to a data processing length of the encryption algorithm corresponding to the plaintext

data block.

[0067] When it is determined that the data length of the plaintext data block is less than or equal to the data processing length of the encryption algorithm corresponding to the plaintext data block, step 202 is performed; and when it is determined that the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, step 204 is performed.

[0068] Step 202: Perform an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result.

[0069] If the data length of the plaintext data block is less than the data processing length of the encryption algorithm corresponding to the plaintext data block, a padding operation may be performed before step 202 is executed.

[0070] Step 203: Encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block.

[0071] At this time, a ciphertext data block generating process for the plaintext data block ends.

[0072] Step 204: Divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length.

[0073] Step 205: Determine a sub ciphertext data block corresponding to each sub plaintext data block. The following manner may be specifically used:

for each sub plaintext data block, sequentially performing an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block.

[0074] Similarly, if a data length of the sub plaintext data block is less than the data processing length, a padding operation may be performed first.

[0075] Operational data corresponding to the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block is the operational data

corresponding to the plaintext data block; and for other sub plaintext data blocks, operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

[0076] Step 206: Combine multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

[0077] Further, operational data corresponding to the first plaintext data block among the multiple plaintext data blocks is preset initial data. In the embodiment of the present invention, for other plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

[0078] Further, in the embodiment of the present invention, when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the following manner may be specifically used to generate the key corresponding to the plaintext data block:

if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is

greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

[0079] The preset parameter value may be a random value, or may be a block number value of the plaintext data block or the like.

[0080] Preferably, the specified sub plaintext data block among the multiple sub plaintext data blocks may specifically be the first sub plaintext data block among the multiple sub plaintext data blocks, or may be the last sub plaintext data block among the multiple sub plaintext data blocks, or may be a sub plaintext data block at another specified position.

[0081] The following describes the foregoing data encryption method provided in the embodiment of the present invention in detail by using a specific example with reference to the accompanying drawings.

[0082] In this example, to-be-encrypted plaintext data P is to be encrypted. A specified length is set, and an entire length interval is divided into two preset length intervals. An encryption algorithm corresponding to a length interval less than or equal to the specified length is a first encryption algorithm with higher security strength, and an encryption algorithm corresponding to a length interval greater than the specified length is a second encryption algorithm with lower security strength. Specifically, a 10-round AES algorithm may be selected as the first encryption algorithm, and a 3-round AES algorithm may be selected as the second encryption algorithm. Data processing lengths of the first encryption algorithm and the second encryption algorithm are both 128 bits. The to-be-encrypted plaintext data P may be divided, by using a preset dividing manner shown in FIG. 3, into plaintext data blocks whose lengths are 128 bits, 256 bits, 128 bits, 256 bits, ..., and it is assumed that ten plaintext data blocks p1, p2, p3, p4, ..., and p10 are obtained.

[0083] For the ten plaintext data blocks p1, p2, p3, p4, ..., and p10, corresponding

ciphertext data blocks are generated sequentially. In this example, 128 bits may be selected as the specified length. Therefore, in the ten plaintext data blocks shown in FIG. 3, an encryption algorithm corresponding to a plaintext data block whose data length is 128 bits is the first encryption algorithm, and an encryption algorithm corresponding to a plaintext data block whose data length is 256 bits is the second encryption algorithm. In addition, because the data processing length of the second encryption algorithm is 128 bits, for a plaintext data block whose data length is 256 bits, the plaintext data block needs to be divided into two sub plaintext data blocks whose data length is 128 bits, sub ciphertext data blocks corresponding to the two sub plaintext data blocks are separately determined, and the sub ciphertext data blocks are combined to obtain a ciphertext data block corresponding to the plaintext data block whose data length is 256 bits.

[0084] A specific ciphertext data block generating manner is shown in FIG. 4.

[0085] For the first plaintext data block p_1 in the ten plaintext data blocks, a corresponding encryption algorithm is a first encryption algorithm ENC-1, corresponding operational data is preset initial data v , a corresponding key is a preset initial key k_1 , and a corresponding preset parameter value is a block number value n_1 of the plaintext data block. A data length of the plaintext data block p_1 is not greater than the data processing length of the first encryption algorithm, and therefore the plaintext data block does not need to be divided into sub plaintext data blocks. An exclusive-or operation is directly performed on the plaintext data block p_1 and the preset initial data v to obtain an operation result, and then the operation result is encrypted based on the first encryption algorithm ENC-1 and by using the preset initial key k_1 , to obtain a ciphertext data block c_1 corresponding to the plaintext data block p_1 .

[0086] The obtained ciphertext data block c_1 may be used as operational data corresponding to the next plaintext data block p_2 . In addition, a key k_2 corresponding to the plaintext data block p_2 may be generated based on the ciphertext data block c_1 . Specifically, an exclusive-or operation is performed on the ciphertext data block c_1 and the block number value n_1 of the plaintext data block to obtain an operation result; and then the operation result is encrypted based on the first encryption algorithm ENC-1 and by using the preset initial key k_1 , to obtain the key k_2 corresponding to the plaintext data block p_2 .

[0087] For the second plaintext data block p_2 , a corresponding encryption algorithm is a second encryption algorithm ENC-2, corresponding operational data is the ciphertext data block c_1 , a corresponding key is the key k_2 , and a corresponding preset parameter value is a block number value n_2 of the plaintext data block. A data length of the plaintext data block p_2 is greater than the data processing length of the second encryption algorithm, and therefore the plaintext data block dividing needs to be performed to obtain two sub plaintext data blocks p_{2_1} and p_{2_2} . For the sub plaintext data block p_{2_1} , corresponding operational data is the operational data corresponding to the plaintext data block p_2 , that is, the ciphertext data block c_1 . An exclusive-or operation is performed on the sub plaintext data block p_{2_1} and the ciphertext data block c_1 to obtain an operation result, and the operation result is encrypted based on the second encryption algorithm ENC-2 and by using the key k_2 , to obtain a sub ciphertext data block c_{2_1} corresponding to the sub plaintext data block p_{2_1} . The obtained sub ciphertext data block c_{2_1} may be used as operational data corresponding to the next sub plaintext data block p_{2_2} . For the sub plaintext data block p_{2_2} , an exclusive-or operation is performed on the sub plaintext data block p_{2_2} and the sub ciphertext data block c_{2_1} to obtain an operation result, and the operation result is encrypted based on the second encryption algorithm ENC-2 and by using the key k_2 , to obtain a sub ciphertext data block c_{2_2} corresponding to the sub plaintext data block p_{2_2} . A ciphertext data block c_2 corresponding to the plaintext data block p_2 is obtained by combining the sub ciphertext data blocks c_{2_1} and c_{2_2} .

[0088] The obtained sub ciphertext data block c_{2_2} may be used as operational data corresponding to the next plaintext data block p_3 . In addition, a key k_3 corresponding to the plaintext data block p_3 may be generated based on the sub ciphertext data block c_{2_2} . Specifically, an exclusive-or operation is performed on the sub ciphertext data block c_{2_2} and the block number value n_2 of the plaintext data block to obtain an operation result; and then the operation result is encrypted based on the second encryption algorithm ENC-2 and by using the key k_2 , to obtain the key k_3 corresponding to the plaintext data block p_3 . In another example of the present invention, the obtained sub ciphertext data block c_{2_1} may also be used as the operational data corresponding to the next plaintext data block p_3 , and the key k_3 corresponding to the plaintext data block p_3 is generated based on the sub ciphertext data

block c2₁.

[0089] Ciphertext data blocks corresponding to the plaintext data blocks p3, p4, ... are generated successively, and a total of ten ciphertext data blocks c1, c2, c3, c4, ..., and c10 are obtained.

5 [0090] Ciphertext data C corresponding to the to-be-encrypted plaintext data P is obtained by combining the ten ciphertext data blocks c1, c2, c3, c4, ..., and c10 in sequence, as shown in FIG. 5.

[0091] It can be seen that, by using the solution provided in the embodiment of the present invention, data encryption is based on different encryption algorithms, which can
10 reduce data encryption duration and improve an overall data processing speed; and a key is generated based on different encryption algorithms, which ensures security of a data encryption method.

[0092] Accordingly, an embodiment of the present invention provides a data decryption method corresponding to the foregoing data encryption method. As shown in FIG. 6, the
15 method includes the following steps:

[0093] Step 601: Divide, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length.

[0094] Step 602: For each ciphertext data block, sequentially determine that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding
20 to a preset length interval within which a data length of the ciphertext data block falls; and generate, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, where a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm
25 corresponding to the preset length interval.

[0095] Step 603: Combine multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted.

[0096] The based preset dividing manner in step 601 is the same as the based preset
30 dividing manner during data encryption; the preset length interval in step 602 is the same as

the preset length interval during data encryption; the decryption algorithm corresponding to the preset length interval corresponds to the encryption algorithm corresponding to the preset length interval during data encryption; and a key corresponding to each ciphertext data block is the same as the key that is used to generate the ciphertext data block during data encryption.

5 [0097] In an embodiment of the present invention, the preset length interval may specifically include two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0098] Further, when the ciphertext data block is the first ciphertext data block among the
10 multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, a key generating manner the same as that used during data encryption is used, that is, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an
15 encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

[0099] Preferably, after the decryption algorithm corresponding to the ciphertext data block is determined in step 602, a specific manner used to generate the plaintext data block corresponding to the ciphertext data block may correspond to the process shown in FIG. 2. As
20 shown in FIG. 7, the following steps are included:

[0100] Step 701: Determine whether the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block.

[0101] When it is determined that the data length of the ciphertext data block is less than
25 or equal to the data processing length of the decryption algorithm corresponding to the ciphertext data block, step 702 is performed; and when it is determined that the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, step 704 is performed.

[0102] Step 702: Decrypt the ciphertext data block based on the decryption algorithm
30 corresponding to the ciphertext data block and by using the key corresponding to the

ciphertext data block, to obtain a decryption result.

[0103] If the data length of the ciphertext data block is less than the data processing length of the decryption algorithm corresponding to the ciphertext data block, a padding operation may be performed before step 702 is executed.

5 [0104] Step 703: Perform an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block.

[0105] At this time, a plaintext data block generating process for the ciphertext data block ends.

10 [0106] Step 704: Divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length.

[0107] Step 705: Determine a sub plaintext data block corresponding to each sub ciphertext data block. The following manner may be specifically used:

for each sub ciphertext data block, sequentially decrypting the sub ciphertext data
15 block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and performing an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block.

20 [0108] Similarly, if a data length of the sub ciphertext data block is less than the data processing length, a padding operation may be performed first.

[0109] Operational data corresponding to the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block is the operational data corresponding to the ciphertext data block; and for other sub ciphertext data blocks,
25 operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

[0110] Step 706: Combine multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

30 [0111] Further, operational data corresponding to the first ciphertext data block among the

multiple ciphertext data blocks is preset initial data. In the embodiment of the present invention, for other ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data
5 corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous
10 ciphertext data block..

[0112] Further, in the embodiment of the present invention, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the following manner may be specifically used to generate the key corresponding to the ciphertext data block:

15 if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, performing an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the
20 encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the
25 previous ciphertext data block, performing an exclusive-or operation on a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext
30 data block and by using the key corresponding to the previous ciphertext data block, to obtain

the key corresponding to the ciphertext data block.

[0113] Preferably, the specified sub ciphertext data block among the multiple sub ciphertext data blocks may specifically be the first sub ciphertext data block among the multiple sub ciphertext data blocks, or may be the last sub ciphertext data block among the multiple sub ciphertext data blocks, or may be a sub ciphertext data block at another specified position.

[0114] The following describes the foregoing data decryption method provided in the embodiment of the present invention in detail by using a specific example with reference to the accompanying drawings.

[0115] In this example, ciphertext data C generated in the foregoing data encryption algorithm example is decrypted. Therefore, the ciphertext data C is divided in a dividing manner that is the same as that used during data encryption. As shown in FIG. 8, The ciphertext data C is divided into ciphertext data blocks whose lengths are 128 bits, 256 bits, 128 bits, 256 bits, ..., and it is assumed that ten ciphertext data blocks c1, c2, c3, c4, ..., and c10 are obtained.

[0116] For the ten ciphertext data blocks c1, c2, c3, c4, ..., and c10, corresponding plaintext data blocks are generated sequentially. Preset length intervals are the same as those set during encryption. Therefore, in the ten ciphertext data blocks shown in FIG. 8, a decryption algorithm corresponding to a ciphertext data block whose data length is 128 bits is a first decryption algorithm, where the first decryption algorithm corresponds to the first encryption algorithm during data encryption; and a decryption algorithm corresponding to a ciphertext data block whose data length is 256 bits is a second decryption algorithm, where the second decryption algorithm corresponds to the second encryption algorithm during data encryption. Data processing lengths of the first decryption algorithm and the second decryption algorithm are both 128 bits. Therefore, for a ciphertext data block whose data length is 256 bits, the ciphertext data block needs to be divided into two sub ciphertext data blocks whose data length is 128 bits, sub plaintext data blocks corresponding to the two sub ciphertext data blocks are separately determined, and the sub plaintext data blocks are combined to obtain a plaintext data block corresponding to the ciphertext data block whose data length is 256 bits.

[0117] A specific plaintext data block generating manner is shown in FIG. 9, which is reverse to the ciphertext data block generating process. A plaintext data block corresponding to each ciphertext data block is generated based on a determined decryption algorithm and by using a key, operational data, and a preset parameter value which are the same as those used during ciphertext data block generating.

[0118] For the first ciphertext data block c1 in the ten ciphertext data blocks, a corresponding decryption algorithm is a first decryption algorithm DEC-1, corresponding operational data is preset initial data v that is the same as that used during encryption, a corresponding key is a preset initial key k1 that is the same as that used during encryption, and a corresponding preset parameter value is a block number value n1 of a plaintext data block. A data length of the ciphertext data block c1 is not greater than the data processing length of the first decryption algorithm, and therefore sub ciphertext data block dividing does not need to be performed. The ciphertext data block c1 is directly decrypted based on the first decryption algorithm DEC-1 and by using the preset initial key k1, to obtain a decryption result, and then an exclusive-or operation is performed on the decryption result and the preset initial data v, to obtain a plaintext data block p1 corresponding to the ciphertext data block c1.

[0119] The ciphertext data block c1 may be used as operational data corresponding to the next ciphertext data block c2. In addition, a key k2 corresponding to the ciphertext data block c2 may be generated based on the ciphertext data block c1 in a generating manner the same as that used during data encryption. Specifically, an exclusive-or operation is performed on the ciphertext data block c1 and the block number value c1 of the ciphertext data block to obtain an operation result; and then the operation result is encrypted based on a first encryption algorithm ENC-1 corresponding to the first decryption algorithm DEC-1 and by using the preset initial key k1, to obtain the key k2 corresponding to the ciphertext data block c2.

[0120] For the second ciphertext data block c2, a corresponding decryption algorithm is a second decryption algorithm DEC-2, corresponding operational data is the ciphertext data block c1, a corresponding key is the key k2, and a corresponding preset parameter value is a block number value n2 of a plaintext data block. A data length of the ciphertext data block c2 is greater than the data processing length of the second decryption algorithm, and therefore ciphertext data block dividing needs to be performed to obtain two sub ciphertext data blocks

c_{2_1} and c_{2_2} . Operational data corresponding to the sub ciphertext data block c_{2_1} is the operational data corresponding to the ciphertext data block c_2 , that is, the ciphertext data block c_1 ; and operational data corresponding to the sub ciphertext data block c_{2_2} is the sub ciphertext data block c_{2_1} . For the sub ciphertext data block c_{2_1} , the sub ciphertext data block c_{2_1} is decrypted based on the second decryption algorithm DEC-2 and by using the key k_2 , to obtain a decryption result, and then an exclusive-or operation is performed on the decryption result and the ciphertext data block c_1 , to obtain a sub plaintext data block p_{2_1} corresponding to the sub ciphertext data block c_{2_1} . For the sub ciphertext data block c_{2_2} , the sub ciphertext data block c_{2_2} is decrypted based on the second decryption algorithm DEC-2 and by using the key k_2 , to obtain a decryption result, and then an exclusive-or operation is performed on the decryption result and the sub ciphertext data block c_{2_1} , to obtain a sub plaintext data block p_{2_2} corresponding to the sub ciphertext data block c_{2_2} . A plaintext data block p_2 corresponding to the ciphertext data block c_2 is obtained by combining the sub plaintext data blocks p_{2_1} and p_{2_2} .

[0121] Similar to data encryption, the sub ciphertext data block c_{2_2} may be used as operational data corresponding to the next ciphertext data block c_3 . In addition, a key k_3 corresponding to the ciphertext data block c_3 may be generated based on the sub ciphertext data block c_{2_2} . Specifically, an exclusive-or operation is performed on the sub ciphertext data block c_{2_2} and the block number value c_2 of the ciphertext data block to obtain an operation result; and then the operation result is encrypted based on the second encryption algorithm ENC-2 corresponding to the second decryption algorithm DEC-2 and by using the key k_2 , to obtain the key k_3 corresponding to the ciphertext data block c_3 .

[0122] Plaintext data blocks corresponding to the ciphertext data blocks c_3 , c_4 , ... are generated successively, and a total of ten plaintext data blocks p_1 , p_2 , p_3 , p_4 , ..., and p_{10} are obtained.

[0123] Plaintext data P corresponding to the ciphertext data C is obtained by combining the ten plaintext data blocks p_1 , p_2 , p_3 , p_4 , ..., and p_{10} in sequence, as shown in FIG. 10.

[0124] Based on a same inventive concept, according to the data encryption method provided in the foregoing embodiment of the present invention, accordingly, an embodiment of the present invention further provides a data encryption apparatus. A schematic structural

diagram of the data encryption apparatus is shown in FIG. 11, and the apparatus specifically includes:

a first dividing unit 1101, configured to divide, based on a preset dividing manner, to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the same data length;

an encrypting unit 1102, configured to sequentially determine, for each plaintext data block, that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext data block falls; and generate, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, where a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval; and

a first combining unit 1103, configured to combine multiple generated ciphertext data blocks according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted.

[0125] Further, the preset length interval specifically includes two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0126] Further, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset initial key; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.

[0127] Further, the encrypting unit 1102 is specifically configured to: when the data length of the plaintext data block is less than or equal to a data processing length of the

encryption algorithm corresponding to the plaintext data block, perform an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially perform an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combine multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

[0128] Further, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext

data block among multiple sub plaintext data blocks of the previous plaintext data block.

[0129] Further, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

[0130] Further, the encrypting unit 1102 is specifically configured to: when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

[0131] Further, the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext

data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

[0132] Functions of the foregoing units may correspond to corresponding processing steps in any one of the processes shown in FIG. 1 to FIG. 5, which are not described in detail herein again.

5 **[0133]** Based on a same inventive concept, according to the data decryption method provided in the foregoing embodiment of the present invention, accordingly, an embodiment of the present invention further provides a data decryption apparatus. A schematic structural diagram of the data decryption apparatus is shown in FIG. 12, and the apparatus specifically includes:

10 a second dividing unit 1201, configured to divide, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length;

a decrypting unit 1202, configured to sequentially determine, for each ciphertext data block, that a decryption algorithm corresponding to the ciphertext data block is a
15 decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generate, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, where a larger value in the preset length interval indicates lower security strength of an encryption algorithm
20 corresponding to the decryption algorithm corresponding to the preset length interval; and

a second combining unit 1203, configured to combine multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted.

25 **[0134]** Further, the preset length interval specifically includes two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

[0135] Further, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a
30 preset initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

[0136] Further, the decrypting unit 1202 is specifically configured to: when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypt the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and perform an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypt the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and perform an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combine multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

[0137] Further, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the

multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

[0138] Further, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

[0139] Further, the decrypting unit 1202 is specifically configured to: when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on a specified sub

ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block.

[0140] Further, the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

[0141] Functions of the foregoing units may correspond to corresponding processing steps in any one of the processes shown in FIG. 6 to FIG. 10, which are not described in detail herein again.

[0142] In conclusion, the solutions provided in the embodiments of the present invention can improve a data processing speed.

[0143] Persons skilled in the art should understand that the embodiments of the present invention may provide a method, a system, or a computer program product. Therefore, the present invention may use a form of a complete hardware embodiment, a complete software embodiment, or an embodiment combining software and hardware. Moreover, the present invention may use a form of a computer program product that is implemented on one or more computer-usable storage mediums (including but not limited to a disk memory, a CD-ROM, an optical memory, and the like) that include computer-usable program code.

[0144] The present invention is described with reference to the flowcharts and/or block diagrams of the method, the device (system), and the computer program product according to the embodiments of the present invention. It should be understood that computer program instructions may be used to implement each process and/or each block in the flowcharts and/or the block diagrams and a combination of a process and/or a block in the flowcharts and/or the block diagrams. These computer program instructions may be provided for a general-purpose computer, a dedicated computer, an embedded processor, or a processor of another programmable data processing device to generate a machine, so that instructions executed by a computer or a processor of another programmable data processing device

generate an apparatus for implementing a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0145] These computer program instructions may also be stored in a computer readable memory that can instruct the computer or another programmable data processing device to work in a specific manner, so that the instructions stored in the computer readable memory generate a manufacture that includes an instruction apparatus. The instruction apparatus implements a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0146] These computer program instructions may also be loaded onto a computer or another programmable data processing device, so that a series of operations and steps are performed on the computer or the another programmable device, thereby generating computer-implemented processing. Therefore, the instructions executed on the computer or the another programmable device provide steps for implementing a specified function in one or more processes in the flowcharts and/or in one or more blocks in the block diagrams.

[0147] Although the exemplary embodiments of the present invention have been described, persons skilled in the art can make changes and modifications to these embodiments once they learn the basic inventive concept. Therefore, the following claims are intended to be construed as to cover the exemplary embodiments and all changes and modifications falling within the scope of the present invention.

[0148] Obviously, persons skilled in the art can make various modifications and variations to the embodiments of the present invention without departing from the spirit and scope of the embodiments of the present invention. Therefore, the present invention is intended to cover these modifications and variations to the embodiments of the present invention provided that these modifications and variations fall within the scope of the claims of the present invention and their equivalent technologies.

CLAIMS

What is claimed is:

1. A data encryption method, comprising:

dividing, based on a preset dividing manner, to-be-encrypted plaintext data into multiple
5 plaintext data blocks that do not have exactly the same data length;

for each plaintext data block, sequentially determining that an encryption algorithm
corresponding to the plaintext data block is an encryption algorithm corresponding to a preset
length interval within which a data length of the plaintext data block falls; and generating,
based on the encryption algorithm corresponding to the plaintext data block and by using a
10 key corresponding to the plaintext data block, a ciphertext data block corresponding to the
plaintext data block, wherein a larger value in the preset length interval indicates lower
security strength of the encryption algorithm corresponding to the preset length interval; and

combining multiple generated ciphertext data blocks according to a sequence of the
multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext
15 data that is obtained after the to-be-encrypted plaintext data is encrypted,

wherein, when the plaintext data block is the first plaintext data block among the
multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset
initial key; and

when the plaintext data block is not the first plaintext data block among the multiple
20 plaintext data blocks, the key corresponding to the plaintext data block is generated according
to a ciphertext data block corresponding to a previous plaintext data block of the plaintext
data block, based on an encryption algorithm corresponding to the previous plaintext data
block, and by using a key corresponding to the previous plaintext data block.

2. The method according to claim 1, wherein the preset length interval specifically
25 comprises two intervals: one preset length interval is a length interval less than or equal to a
specified length, and the other preset length interval is a length interval greater than the
specified length.

3. The method according to any one of claims 1 to 2, wherein the generating, based on the encryption algorithm corresponding to the plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block specifically comprises:

5 when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, performing an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key
10 corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

 when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, dividing the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to
15 the data processing length; for each sub plaintext data block, sequentially performing an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypting the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block
20 corresponding to the sub plaintext data block; and combining multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

4. The method according to claim 3, wherein, when the plaintext data block is the first
25 plaintext data block among the multiple plaintext data blocks, the operational data corresponding to the plaintext data block is preset initial data; and

 when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm
30 corresponding to the previous plaintext data block, the operational data corresponding to the

plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

5 5. The method according to claim 3, wherein, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

10 when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

15 6. The method according to claim 3, wherein the key corresponding to the plaintext data block is generated specifically in the following manner:

20 when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

25 if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, performing an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to

30

the previous plaintext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

5 7. The method according to claim 4 or 67, wherein the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

8. A data decryption method, comprising:

10 dividing, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length;

for each ciphertext data block, sequentially determining that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, wherein a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm corresponding to the preset length interval; and

15

20 combining multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted,

wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset initial key; and

25

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

30

9. The method according to claim 8, wherein the preset length interval specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

10. The method according to any one of claims 8 to 9, wherein the generating, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block specifically comprises:

when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypting the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and performing an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, dividing the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypting the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and performing an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combining multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

11. The method according to claim 10, wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

12. The method according to claim 10, wherein, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the sub ciphertext data block.

13. The method according to claim 10, wherein the key corresponding to the ciphertext data block is generated specifically in the following manner:

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, performing an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block; and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the

previous ciphertext data block, performing an exclusive-or operation on a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypting the operation result based on the encryption
5 algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain the key corresponding to the ciphertext data block.

14. The method according to claim 11 or 13, wherein the specified sub ciphertext data block among the multiple sub ciphertext data blocks is specifically the first sub ciphertext
10 data block among the multiple sub ciphertext data blocks or the last sub ciphertext data block among the multiple sub ciphertext data blocks.

15. A data encryption apparatus, comprising:

a first dividing unit, configured to divide, based on a preset dividing manner, to-be-encrypted plaintext data into multiple plaintext data blocks that do not have exactly the
15 same data length;

an encrypting unit, configured to sequentially determine, for each plaintext data block, that an encryption algorithm corresponding to the plaintext data block is an encryption algorithm corresponding to a preset length interval within which a data length of the plaintext data block falls; and generate, based on the encryption algorithm corresponding to the
20 plaintext data block and by using a key corresponding to the plaintext data block, a ciphertext data block corresponding to the plaintext data block, wherein a larger value in the preset length interval indicates lower security strength of the encryption algorithm corresponding to the preset length interval; and

a first combining unit, configured to combine multiple generated ciphertext data blocks according to a sequence of the multiple plaintext data blocks that are obtained by means of the dividing, to obtain ciphertext data that is obtained after the to-be-encrypted plaintext data is encrypted,
25

wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is a preset
30 initial key; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, the key corresponding to the plaintext data block is generated according to a ciphertext data block corresponding to a previous plaintext data block of the plaintext data block, based on an encryption algorithm corresponding to the previous plaintext data block, and by using a key corresponding to the previous plaintext data block.

16. The apparatus according to claim 15, wherein the preset length interval specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

17. The apparatus according to any one of claims 15 to 16, wherein the encrypting unit is specifically configured to: when the data length of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the plaintext data block, perform an exclusive-or operation on the plaintext data block and operational data corresponding to the plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain the ciphertext data block corresponding to the plaintext data block; and

when the data length of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the plaintext data block, divide the plaintext data block into multiple sub plaintext data blocks whose data length is less than or equal to the data processing length; for each sub plaintext data block, sequentially perform an exclusive-or operation on the sub plaintext data block and operational data corresponding to the sub plaintext data block, to obtain an operation result, and encrypt the operation result based on the encryption algorithm corresponding to the plaintext data block and by using the key corresponding to the plaintext data block, to obtain a sub ciphertext data block corresponding to the sub plaintext data block; and combine multiple obtained sub ciphertext data blocks according to a sequence of the multiple sub plaintext data blocks that are obtained by means of the dividing, to obtain the ciphertext data block corresponding to the plaintext data block.

18. The apparatus according to claim 17, wherein, when the plaintext data block is the first plaintext data block among the multiple plaintext data blocks, the operational data

corresponding to the plaintext data block is preset initial data; and

when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is the ciphertext data block corresponding to the previous plaintext data block; and if the data length of the previous plaintext data block of the plaintext data block is greater than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, the operational data corresponding to the plaintext data block is a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block.

19. The apparatus according to claim 17, wherein, when the sub plaintext data block is the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is the operational data corresponding to the plaintext data block; and

when the sub plaintext data block is not the first sub plaintext data block among the multiple sub plaintext data blocks of the plaintext data block, the operational data corresponding to the sub plaintext data block is a sub ciphertext data block corresponding to a previous sub plaintext data block of the sub plaintext data block.

20. The apparatus according to claim 17, wherein the encrypting unit is specifically configured to: when the plaintext data block is not the first plaintext data block among the multiple plaintext data blocks, if a data length of the previous plaintext data block of the plaintext data block is less than or equal to a data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on the ciphertext data block corresponding to the previous plaintext data block and a preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block; and

if the data length of the previous plaintext data block of the plaintext data block is greater

than the data processing length of the encryption algorithm corresponding to the previous plaintext data block, perform an exclusive-or operation on a sub ciphertext data block corresponding to a specified sub plaintext data block among multiple sub plaintext data blocks of the previous plaintext data block and the preset parameter value corresponding to the previous plaintext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the previous plaintext data block and by using the key corresponding to the previous plaintext data block, to obtain the key corresponding to the plaintext data block.

21. The apparatus according to claim 18 or 20, wherein the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.

22. A data decryption apparatus, comprising:

a second dividing unit, configured to divide, based on a preset dividing manner, to-be-decrypted ciphertext data into multiple ciphertext data blocks that do not have exactly the same data length;

a decrypting unit, configured to sequentially determine, for each ciphertext data block, that a decryption algorithm corresponding to the ciphertext data block is a decryption algorithm corresponding to a preset length interval within which a data length of the ciphertext data block falls; and generate, based on the decryption algorithm corresponding to the ciphertext data block and by using a key corresponding to the ciphertext data block, a plaintext data block corresponding to the ciphertext data block, wherein a larger value in the preset length interval indicates lower security strength of an encryption algorithm corresponding to the decryption algorithm corresponding to the preset length interval; and

a second combining unit, configured to combine multiple decrypted plaintext data blocks according to a sequence of the multiple ciphertext data blocks that are obtained by means of the dividing, to obtain plaintext data that is obtained after the to-be-decrypted ciphertext data is decrypted,

wherein, when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is a preset

initial key; and

when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, the key corresponding to the ciphertext data block is generated according to a previous ciphertext data block of the ciphertext data block, based on an encryption algorithm corresponding to a decryption algorithm corresponding to the previous ciphertext data block, and by using a key corresponding to the previous ciphertext data block.

23. The apparatus according to claim 22, wherein the preset length interval specifically comprises two intervals: one preset length interval is a length interval less than or equal to a specified length, and the other preset length interval is a length interval greater than the specified length.

24. The apparatus according to any one of claims 22 to 23, wherein the decrypting unit is specifically configured to: when the data length of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the ciphertext data block, decrypt the ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result; and perform an exclusive-or operation on the decryption result and operational data corresponding to the ciphertext data block, to obtain the plaintext data block corresponding to the ciphertext data block; and

when the data length of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the ciphertext data block, divide the ciphertext data block into multiple sub ciphertext data blocks whose data length is less than or equal to the data processing length; for each sub ciphertext data block, sequentially decrypt the sub ciphertext data block based on the decryption algorithm corresponding to the ciphertext data block and by using the key corresponding to the ciphertext data block, to obtain a decryption result, and perform an exclusive-or operation on the decryption result and operational data corresponding to the sub ciphertext data block, to obtain a sub plaintext data block corresponding to the sub ciphertext data block; and combine multiple obtained sub plaintext data blocks according to a sequence of the multiple sub ciphertext data blocks that are obtained by means of the dividing, to obtain the plaintext data block corresponding to the ciphertext data block.

25. The apparatus according to claim 24, wherein, when the ciphertext data block is the first ciphertext data block among the multiple ciphertext data blocks, the operational data corresponding to the ciphertext data block is preset initial data; and

when the ciphertext data block is not the first ciphertext data block among the multiple
5 ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is the previous ciphertext data block; and if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing
10 length of the decryption algorithm corresponding to the previous ciphertext data block, the operational data corresponding to the ciphertext data block is a specified sub ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block.

26. The apparatus according to claim 24, wherein, when the sub ciphertext data block is the first sub ciphertext data block among the multiple sub ciphertext data blocks of the
15 ciphertext data block, the operational data corresponding to the sub ciphertext data block is the operational data corresponding to the ciphertext data block; and

when the sub ciphertext data block is not the first sub ciphertext data block among the multiple sub ciphertext data blocks of the ciphertext data block, the operational data corresponding to the sub ciphertext data block is a previous sub ciphertext data block of the
20 sub ciphertext data block.

27. The apparatus according to claim 24, wherein the decrypting unit is specifically configured to: when the ciphertext data block is not the first ciphertext data block among the multiple ciphertext data blocks, if a data length of the previous ciphertext data block of the ciphertext data block is less than or equal to a data processing length of the decryption
25 algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on the previous ciphertext data block and a preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the
30 previous ciphertext data block, to obtain the key corresponding to the ciphertext data block;

and

if the data length of the previous ciphertext data block of the ciphertext data block is greater than the data processing length of the decryption algorithm corresponding to the previous ciphertext data block, perform an exclusive-or operation on a specified sub
5 ciphertext data block among multiple sub ciphertext data blocks of the previous ciphertext data block and the preset parameter value corresponding to the previous ciphertext data block, to obtain an operation result; and encrypt the operation result based on the encryption algorithm corresponding to the decryption algorithm corresponding to the previous ciphertext data block and by using the key corresponding to the previous ciphertext data block, to obtain
10 the key corresponding to the ciphertext data block.

28. The apparatus according to claim 25 or 27, wherein the specified sub plaintext data block among the multiple sub plaintext data blocks is specifically the first sub plaintext data block among the multiple sub plaintext data blocks or the last sub plaintext data block among the multiple sub plaintext data blocks.