

[0034]

A main object of the present invention is to provide an analysis system and the like that are able to efficiently extract, from second data, in accordance with a specific criterion, a candidate of a correct encryption
5 key which first data encrypted by a specific encryption scheme can be decrypted (decoded). For example, the first data may be the aforementioned encrypted communication data. Further, for example, the second data may be data stored in the aforementioned memory space.

[Solution to Problem]

10 [0035]

An analysis system according to one aspect of the present invention includes: cryptanalysis means including: key candidate extraction means for
15 extracting, from second data, one or more candidates of key data that include an encryption key by which first data encrypted by a specific encryption scheme can be decrypted, based on data indicating a feature of the key data; and decryption means for extracting, from the extracted candidates of key data, correct key data by which the encrypted first data
20 can be correctly decrypted, based on a result of decrypting the first data by use of the extracted candidates of key data, wherein the key candidate extraction means extracts, from the second data, one or more of the candidates of key data, based on key candidate determination information including the encryption scheme, and a key candidate determination criterion including information that enables to extract the candidate of key data from the second data based on the data indicating the feature of the key data used in the encryption scheme.

[0036]

An analysis method according to one
25 aspect includes: by an information processing

apparatus, extracting, from second data, one or more candidates of key data that include an encryption key by which first data encrypted by a specific encryption scheme can be decrypted, based on data indicating a feature of the key data; and extracting, from one or more of the candidates of key

data, correct key data by which the encrypted first data can be correctly decrypted, based on a result of decrypting the first data by use of the extracted candidates of key data, wherein

the step of extracting, from the second data, comprises extracting one or more of the candidates of key data, based on key candidate determination information including the encryption scheme, and a key candidate determination criterion including information that enables to extract the candidate of key data from the second data based on the data indicating the feature of the key data used in the encryption scheme.

[0037]

- 5 Further, the object is also achieved by an analysis system including the aforementioned configuration, a computer program providing a corresponding analysis method by a computer, and a computer readable storage medium and the like storing the computer program.

[Advantageous Effects of Invention]

10 [0038]

The present invention enables to efficiently extract, from second data, in accordance with a specific criterion, a candidate of a correct encryption key which first data encrypted by a specific encryption scheme can be decrypted (decoded).

15 [Brief Description of Drawings]

[0039]

[Fig. 1] Fig. 1 is a block diagram illustrating functional configurations of an analysis system, an analysis target apparatus, and the like, according to a first example embodiment of the present invention.

20 [Fig. 2] Fig. 2 is a diagram illustrating a first configuration example capable of providing the analysis target apparatus and a memory acquisition unit, according to the first example embodiment of the present invention.

[Fig. 3] Fig. 3 is a diagram illustrating a second configuration

25 example capable of providing the analysis target apparatus and the memory acquisition unit, according to the first example embodiment of the present invention.

[Fig. 4] Fig. 4 is a diagram illustrating a specific example of a key data acquisition policy according to the first example embodiment of the

CLAIMS:

1. An analysis system comprising cryptanalysis means including:

key candidate extraction means for extracting, from second data, one or more candidates of key data that include an encryption key that enables to decrypt first data encrypted by a specific encryption scheme, based on data indicating a feature of the key data; and

decryption means for extracting, from the extracted candidates of key data, correct key data that enables to correctly decrypt the encrypted first data, based on a result of decrypting the first data by use of the extracted candidates of key data.

wherein

the key candidate extraction means extracts, from the second data, one or more of the candidates of key data, based on key candidate determination information including the encryption scheme, and a key candidate determination criterion including information that enables to extract the candidate of key data from the second data based on the data indicating the feature of the key data used in the encryption scheme.

2. The analysis system according to Claim 1, wherein

the data indicating the feature of the key data and the key candidate determination criterion are any one of

the data indicating the feature of the key data representing entropy of specific data included in the second data, and the key candidate determination criterion including information that enables to determine whether to extract the specific data as the candidate of key data based on the entropy;

the data indicating the feature of the key data representing a value of specific data included in the second data, and the key candidate determination criterion including information that enables to determine whether to extract the specific data as the candidate of key data based on whether the specific data include a predetermined value; and

the data indicating the feature of the key data representing data indicating a placement pattern of specific data included in the second data, and the key candidate determination criterion

including information that enables to determine whether to extract the specific data as the candidate of key data based on the data indicating the placement pattern.

3. The analysis system according to Claim 1 or Claim 2, wherein
the key candidate determination information further includes at least one of an encryption parameter at least including a size of the key and an encryption mode used in the encryption scheme, and information indicating an execution environment of processing with regard to the encryption scheme in the information communication apparatus.
4. The analysis system according to any one of Claims 1 to 3, wherein,
for each of the one or more extracted candidates of key data, the decryption means determines whether the first data are correctly decrypted by the candidate of key data, by use of analysis result determination information that enables to determine whether the first data is successfully decrypted or not based on data indicating a feature of decrypted data that is a result of decrypting the first data.
5. The analysis system according to Claim 4, wherein
the data indicating the feature of decrypted data and the analysis result determination information are any one of:
the data indicating the feature of decrypted data representing entropy of the decrypted data, and the analysis result determination information including information that enables to determine whether the first data is successfully decrypted or not based on entropy of the decrypted data;
the data indicating the feature of decrypted data representing value of specific data included in the decrypted data, and the analysis result determination information including information that enables to determine whether the first data is successfully decrypted or not based on whether the decrypted data include the value of specific data; and
the data indicating the feature of the decrypted data representing data indicating a data format of the decrypted data, and the analysis result determination information including information that enables to determine whether the first data is successfully decrypted or not based on whether the data format of the decrypted data conforms to a specific data format.

6. The analysis system according to any one of Claims 1 to 2, wherein
the key candidate determination information further includes information that enables to extract a candidate of encryption processing data, being used with the encryption key when decrypting the first data encrypted by the specific encryption scheme, from the second data based on a feature of the encryption processing data, and
the key candidate extraction means extracts one or more of the candidates of the encryption processing data from the second data based on the key candidate determination information.
7. The analysis system according to Claim 6, wherein
the key candidate extraction means selects, for each of the encryption schemes, an area to be searched when extracting, from the second data, at least one of the candidate of key data and the candidate of encryption processing data, based on the key candidate determination information.
8. An analysis method comprising, by an information processing apparatus:
extracting, from second data, one or more candidates of key data that include an encryption key that enables to decrypt first data encrypted by a specific encryption scheme, based on data indicating a feature of the key data; and
extracting, from one or more of the candidates of key data, correct key data that enables to correctly decrypt the encrypted first data, based on a result of decrypting the first data by use of the extracted candidates of key data, wherein
the step of extracting, from the second data, comprises extracting one or more of the candidates of key data, based on key candidate determination information including the encryption scheme, and a key candidate determination criterion including information that enables to extract the candidate of key data from the second data based on the data indicating the feature of the key data used in the encryption scheme.
9. A non-transitory computer-readable storage medium storing a computer program allowing a computer to execute:

94a

processing of extracting, from second data, one or more candidates of key data that include an encryption key that enables to decrypt first data encrypted by a specific encryption scheme, based on data indicating a feature of the key data; and

processing of extracting, from one or more of the candidates of key data, correct key data that enables to correctly decrypt the encrypted first data, based on a result of decrypting the first data by use of the extracted candidates of key data.