

[Document Name] DESCRIPTION**[Title of Invention] ANALYSIS SYSTEM, ANALYSIS METHOD, AND STORAGE MEDIUM**5 **[Technical Field]**

 [0001]

 The present invention relates to a technology of analyzing cryptographic communication executed by an information communication apparatus and the like.

10 **[Background Art]**

 [0002]

 There is a demand for a technology of analyzing communication processing executed by an information processing apparatus (such as a computer) that is connected to a communication network (hereinafter simply referred to as an “information communication apparatus”), in recent years.

 [0003]

 For example, such analysis of communication processing is used for analysis of behavior of an information communication apparatus during development and operation stages, or analysis of behavior of a communication processing program executed on an information communication apparatus.

 [0004]

 There is a particular demand in recent years for a technology for analyzing a content of improper communication processing caused by an improper computer program (a computer program includes various types of software programs, and may be hereinafter simply referred to as a “program”), such as a virus, that is executed on an information communication apparatus.

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.
2. The analysis system according to Claim 1, 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.
3. The analysis system according to Claim 2, 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.

4. The analysis system according to Claim 2 or Claim 3, 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.
5. The analysis system according to any one of Claims 1 to 4, 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.
6. The analysis system according to Claim 5, 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.

7. The analysis system according to any one of Claims 2 to 6, 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.
8. The analysis system according to Claim 7, 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.
9. 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.
10. A non-transitory computer-readable storage medium storing a computer program allowing a computer to execute:
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.