

[Title of Invention] ANALYSIS SYSTEM, ANALYSIS DEVICE,
ANALYSIS METHOD, AND STORAGE MEDIUM HAVING ANALYSIS
PROGRAM RECORDED THEREIN

[Document Name] ABSTRACT

In order to extract encryption key candidates capable of
deciphering (decoding) first data encrypted using a specified encryption
method, from second data on the basis of a specified standard, this analysis
5 system comprises an encryption analysis means having: a key candidate
extraction unit that extracts at least one key data candidate including
encryption keys capable of deciphering first data encrypted using the
specified encryption method, from the second data on the basis of data
indicating the characteristics of the key data; and an encryption
10 deciphering means that extracts the correct key data capable of correctly
deciphering the encrypted first data, from the at least one key data
candidate, on the basis of the results of deciphering of the first data using
the extracted key data candidates.

[Fig. 17A]