Search for a tool

Results

dCode's analyzer suggests to investigate:

	↑↓	↑↓
ASCII Shift Cipher		■■■■■■■■
ASCII Code		■■
XOR Cipher		■
Base62 Encoding		■
Base64 Coding		■
Circular Bit Shift		■
Hexadecimal (Base 16)		■
EBCDIC Encoding		■
RC4 Cipher		■
Huffman Coding		■
LZW Compression		■
Substitution Cipher		■
Octal System (Base 8)		■
Shift Cipher		□
Keyboard Coordinates		□
Homophonic Cipher		□
URL Decoder		□

#17

CIPHER IDENTIFIER

Cryptography › **Cipher Identifier**

ENCRYPTED MESSAGE IDENTIFIER ↻

CIPHERTEXT TO RECOGNIZE (?)

```
4e 44 4a 43 51 30 35 37 59 6a 51 31 4d 31 38 32 4e 46 38 78
4e 56 39 6a 4d 44 42 73 58 32 4a 31 4e 31 39
6f 4d 33 68 66 4d 54 56 66 59 7a 41 77 62 44 4e 79 66 51 3d
3d
```

CLUES/KEYWORDS (IF ANY) _____

▶ ANALYZE

See also: **Frequency Analysis** — **Index of Coincidence**

SYMBOLS IDENTIFIER

▫ *Go to:* **Symbols Cipher List**

Answers to Questions (FAQ)

What is a cipher identifier? (Definition)

A encryption detector is a computer tool designed to recognize encryption/encoding from a text message. The detector performs cryptanalysis, examines various features of the text, such as letter distribution, character repetition, word length, etc. to determine the type of encryption and guide users to the right tools based on the type of code or encryption identified.

How to decrypt a cipher text?

To decrypt / decipher an encoded message, it is necessary to know the encryption used (or the encoding method, or the implemented cryptographic principle). Without knowing the technique chosen by the sender of the message, it is impossible to decrypt it (or decode it). Knowing the encryption (or encoding, or code) is therefore the first step to start the decryption (or decoding) process.

dCode therefore proposes, on this page above, an artificial intelligence tool dedicated to the automatic recognition/identification of encryption and direct links to tools capable of deciphering the message/text.

How to recognize a cipher?

To recognize/guess the type of encryption/encoding used to encrypt/encode a message, dCode uses several detection/cryptanalysis methods:

— **frequency analysis**: which characters of the message appear most often? In what proportion? Which characters do not appear? This analysis can

be carried out for all the characters (but often the letters A–Z and the numbers 0–9 allow to eliminate many methods of ciphers/coding). The analysis of **bigrams** or **trigrams** (or more generally group of letters) makes it possible to refine the cryptanalysis, the presence or absence of certain groups of letters are clues.

— the **coincidence index**: how random are the characters of the message? Intelligible messages (in English) tend to favor certain letters and do not use the E in the same way as the X (much rarer).

— signature search: certain ciphers / encodings have characteristic marks, a signature which makes them identifiable.

Example: The **base64** code contains all the possible numbers and letters (**upper and lower case**) distributed fairly evenly but 3 times out of 4, it ends with the sign =.

When the message is accompanied by instructions or clues, some keywords can trigger more results from the dCode database. NB: do not indicate known plaintext.

Why does the detector display a warning?

Sometimes the **cipher identifier** finds little or no relevant result, several reasons are possible:

— The message is too short: a message containing not enough characters does not allow a good **frequency analysis** to be performed. The possibilities become very numerous without a way to precisely identify the encryption.

— The message has a low entropy: it is composed of few distinct characters (a binary message containing only 0s and 1s has a low entropy). Furthermore, nearly all messages can be stored **in binary**, identifying the encryption precisely is difficult.

— The message contains unnecessary characters (such as spaces between each letter), which weakens the frequency analyses. Remove spaces or other unnecessary symbols for best results.

— The message is over-encrypted: several successive encodings / ciphers have been applied, the over-encryption tends to mask the characteristic signatures of the original encryption.

— The message is composed of several distinct messages: the presence of several ciphers with different properties disturbs the detector which searches for a single cipher. Please **split the message** to determine the coding of each portion.

— The encryption used is recent: modern cryptography techniques are such that it is impossible to recognize an encrypted message from a random message, it is moreover a quality of a good encryption. Identification is, in essence, difficult.

— The encryption used is very rare: dCode can detect more than 300 different ciphers and continues to improve thanks to your feedback and messages, but it is not impossible that some ciphers are still unknown/missing.

Why does the analyzer/recognizer not detect my cipher method?

Sometimes the recognizer algorithm (based on artificial intelligence and machine learning) finds multiple signals, distinctive signs from several cipher types, and returns approximate results. Please contact us with your cipher message, the original message and the encryption method used so that dCode can *teach* the analyzer/finder this encryption for future times. The more data there is, the more accurate the detection will be.

How does the cipher identifier work?

The program is based on a neural network type architecture, more precisely a multilayer perceptron (MLP). At the input layer there are the coded messages (with ngrams), and at the output layer the different types of known and referenced ciphers on dCode. Regularly the database is updated and new ciphers are added which allows to refine the results.

ASK A NEW QUESTION

Source code

dCode retains ownership of the "Cipher Identifier" source code. Except explicit open source licence (indicated Creative Commons / free), the "Cipher Identifier" algorithm, the applet or snippet (converter, solver, encryption / decryption, encoding / decoding, ciphering / deciphering, breaker, translator), or the "Cipher Identifier" functions (calculate, convert, solve, decrypt / encrypt, decipher / cipher, decode / encode, translate) written in any informatic language (Python, Java, PHP, C#, Javascript, Matlab, etc.) and all data download, script, or API access for "Cipher Identifier" are not public, same for offline use on PC, mobile, tablet, iPhone or Android app!
Reminder : dCode is free to use.

Cita dCode

The copy-paste of the page "Cipher Identifier" or any of its results, is allowed (even for commercial purposes) as long as you cite dCode!
Exporting results as a .csv or .txt file is free by clicking on the *export* icon
Cite as source (bibliography):
Cipher Identifier on dCode.fr [online website], retrieved on 2024-01-18,
https://www.dcode.fr/cipher-identifier