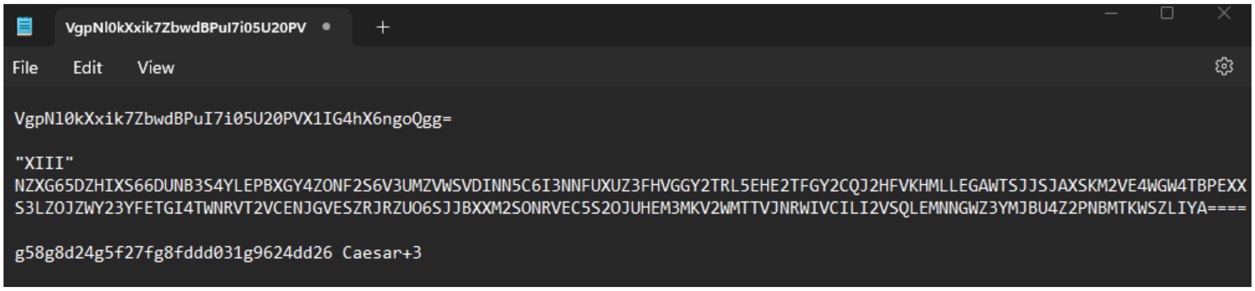
2023

CTF #5

GROUP NUMBER: 3

GROUP MEMBERS NAMES: **Noah Stacy, Sam Seggie, Dillon Kelly, Patrick Palcic, Aidan Pfiefer**

Figure 1



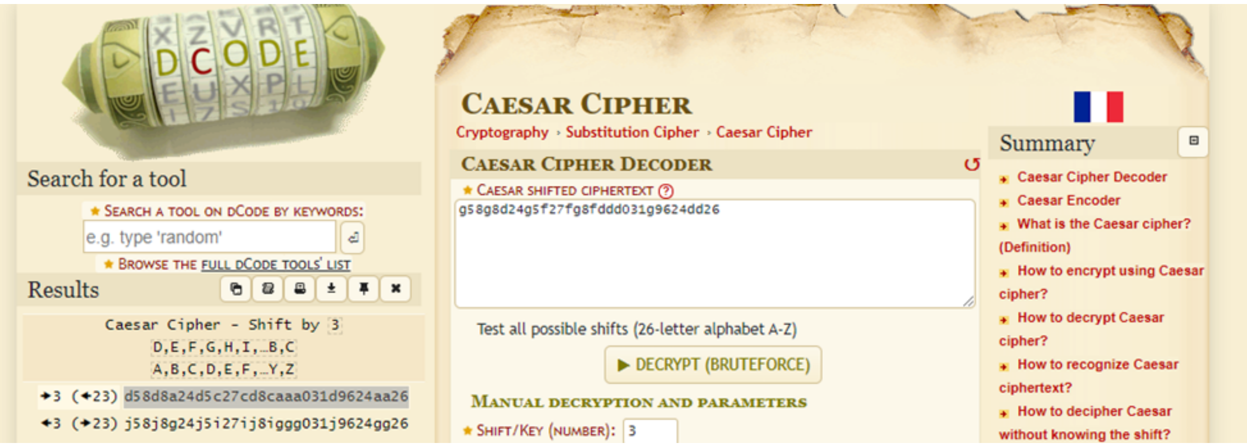
```
VgpNl0kXxik7ZbwdBPuI7i05U20PVX1IG4hX6ngoQgg=

"XIII"
NZXG65DZHIXS66DUNB3S4YLEPBXGY4ZONF2S6V3UMZVWSVDINN5C6I3NNFUXUZ3FHVGGY2TRL5EHE2TFGY2CQJ2HFVKHMLLEGAWTSJJSJAXSKM2VE4WGW4TBPEXX
S3LZOJZWY23YFETGI4TWNRVT2VCENJGVESZRJRZUO6SJJBXXM2SONRVEC5S2OJUHEM3MKV2WMTTVJNRWIVCILI2VSQLEMNNGWZ3YMJBU4Z2PNBMTKWSZLIYA====

g58g8d24g5f27fg8fddd031g9624dd26 Caesar+3
```

After retrieving the decoded messages from the steganographic decoding tool, we then decided to put each of the codes into the code analyzer to analyze what kind of encoding was done. Starting with the string of code with “Caesar+3” at the end, we simply copy and pasted the code into Google with the word “decode” after. Upon searching this, we saw the Caesar Cipher decoding technique [1]. When we put in the string, it provided us with two options. The second option didn’t come up with a valid decoding process (Figure 2A). However, the first option brought us to MD5 (hash) as noted by the cipher identifier (Figure 2B). We then decoded the hash, giving us a message that says “notevenclose” (Figure 2C).

Figure 2A



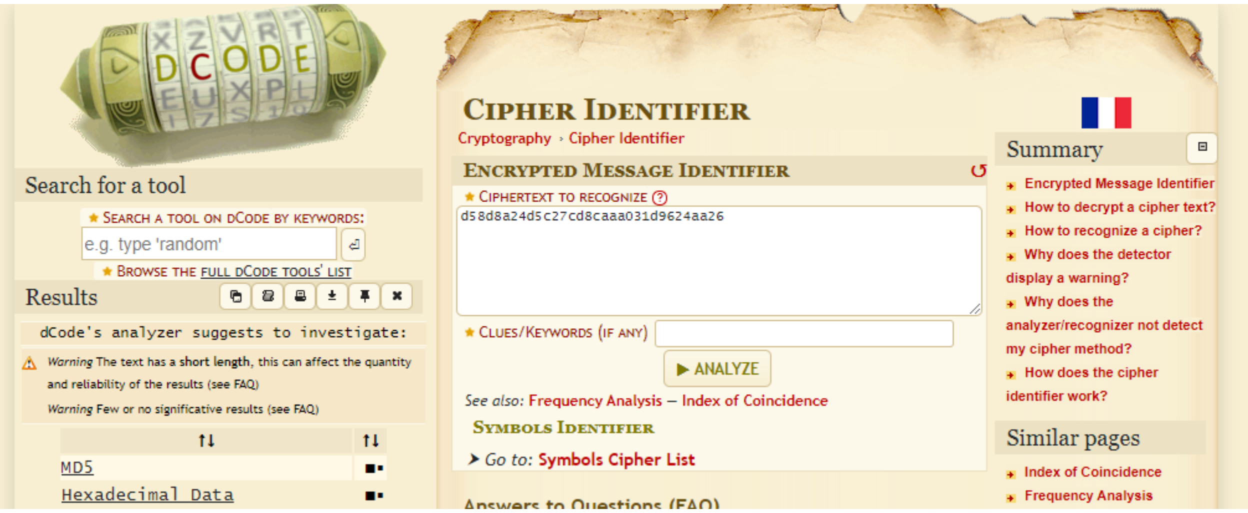
DCODE
Search for a tool
★ SEARCH A TOOL ON DCODE BY KEYWORDS:
e.g. type 'random'
★ BROWSE THE FULL DCODE TOOLS' LIST
Results
CAESAR CIPHER
Cryptography › Substitution Cipher › Caesar Cipher
CAESAR CIPHER DECODER
Test all possible shifts (26-letter alphabet A-Z)
▶ DECRYPT (BRUTEFORCE)
MANUAL DECRYPTION AND PARAMETERS
Summary
Caesar Cipher Decoder
Caesar Encoder
What is the Caesar cipher? (Definition)
How to encrypt using Caesar cipher?
How to decrypt Caesar cipher?
How to recognize Caesar ciphertext?
How to decipher Caesar without knowing the shift?

```
Caesar Cipher - Shift by 3
D,E,F,G,H,I,…B,C
A,B,C,D,E,F,…Y,Z
→3 (←23) d58d8a24d5c27cd8caaa031d9624aa26
←3 (→23) j58j8g24j5i27ij8iggg031j9624gg26
```

★ CAESAR SHIFTED CIPHERTEXT: g58g8d24g5f27fg8fddd031g9624dd26

★ SHIFT/KEY (NUMBER): 3

Figure 2B


Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'random'
★ Browse the full dCode tools' list
Results
Cipher Identifier
Cryptography › Cipher Identifier
Encrypted Message Identifier
★ Ciphertext to recognize
★ Clues/Keywords (if any)
▶ ANALYZE
See also: Frequency Analysis – Index of Coincidence
Symbols Identifier
➤ Go to: Symbols Cipher List
Answers to Questions (FAQ)
Summary
Encrypted Message Identifier
How to decrypt a cipher text?
How to recognize a cipher?
Why does the detector display a warning?
Why does the analyzer/recognizer not detect my cipher method?
How does the cipher identifier work?
Similar pages
Index of Coincidence
Frequency Analysis

```
d58d8a24d5c27cd8caaa031d9624aa26
```

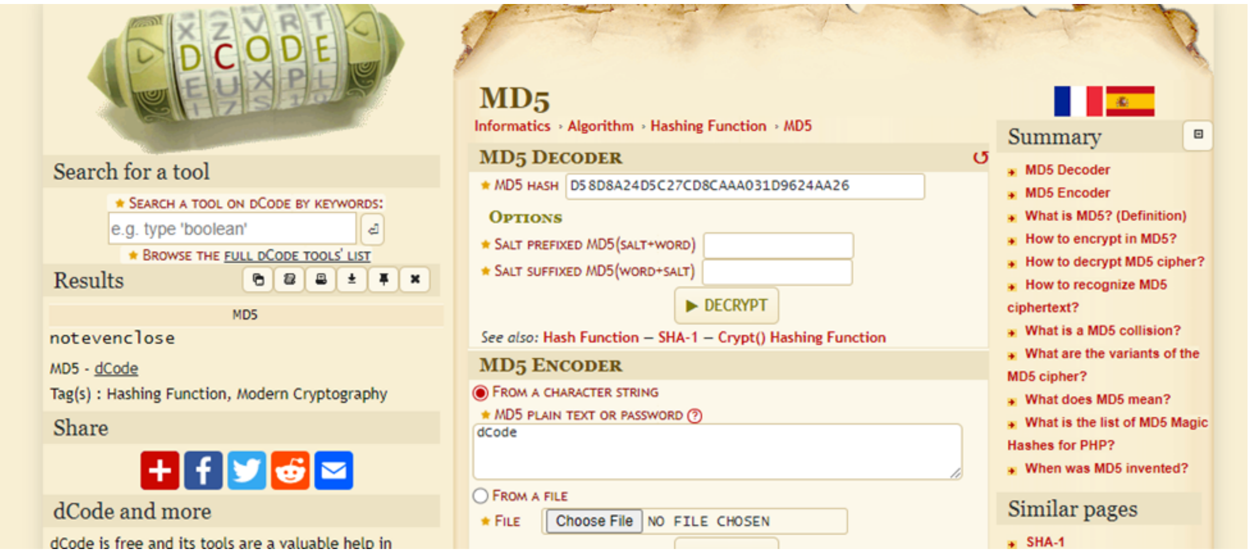
dCode's analyzer suggests to investigate:

⚠ *Warning* The text has a short length, this can affect the quantity and reliability of the results (see FAQ)

Warning Few or no significative results (see FAQ)

↑↓	↑↓
MD5	■▪
Hexadecimal Data	■▪

Figure 2C


Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'boolean'
★ Browse the full dCode tools' list
Results
Share
dCode and more
MD5
Informatics › Algorithm › Hashing Function › MD5
MD5 Decoder
Options
★ Salt prefixed MD5(salt+word)
★ Salt suffixed MD5(word+salt)
▶ DECRYPT
See also: Hash Function – SHA-1 – Crypt() Hashing Function
MD5 Encoder
★ MD5 plain text or password
○ From a file
★ File
Choose File
Summary
MD5 Decoder
MD5 Encoder
What is MD5? (Definition)
How to encrypt in MD5?
How to decrypt MD5 cipher?
How to recognize MD5 ciphertext?
What is a MD5 collision?
What are the variants of the MD5 cipher?
What does MD5 mean?
What is the list of MD5 Magic Hashes for PHP?
When was MD5 invented?
Similar pages
SHA-1

★ MD5 hash: D58D8A24D5C27CD8CAAA031D9624AA26

● From a character string

★ MD5 plain text or password: dCode

File: NO FILE CHOSEN

MD5

```
notevenclose
```

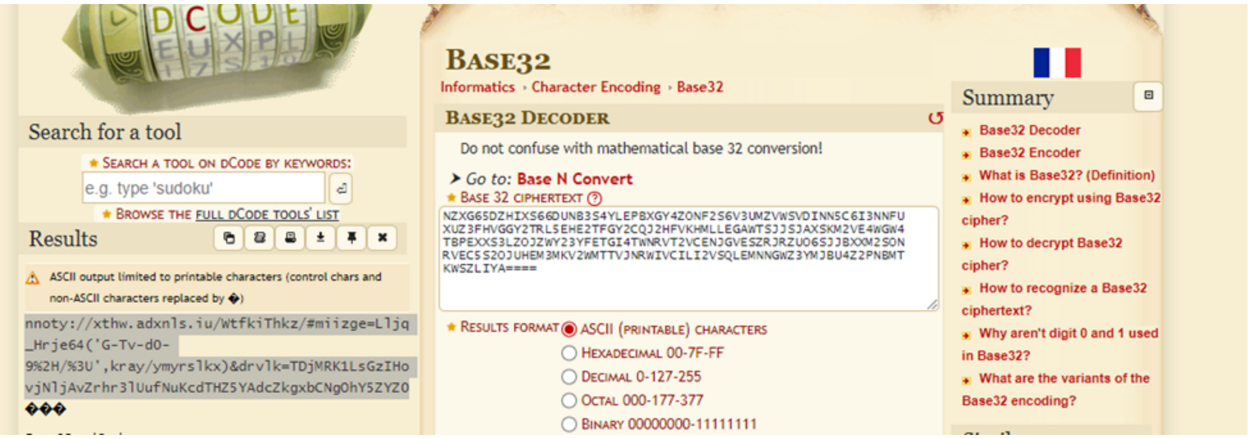
MD5 - dCode

Tag(s) : Hashing Function, Modern Cryptography

dCode is free and its tools are a valuable help in

Moving on, the second string in the list led us to using a Base32 decoder [1]. Copying the full string with the “XIII” in the beginning led to jumbled letters and numbers. When taking out the “XIII,” we got the full result we needed. The Base32 decoder shows below what appears to be a link to somewhere, though it itself is obfuscated (Figure 3).

Figure 3


D C O D E
E U X P L
Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'sudoku'
★ Browse the full dCode tools' list
Results
Base32
Informatics › Character Encoding › Base32
Summary
Base32 Decoder
Base32 Encoder
What is Base32? (Definition)
How to encrypt using Base32 cipher?
How to decrypt Base32 cipher?
How to recognize a Base32 ciphertext?
Why aren't digit 0 and 1 used in Base32?
What are the variants of the Base32 encoding?

ASCII output limited to printable characters (control chars and non-ASCII characters replaced by �)

```
nnoty://xthw.adxnls.iu/WtfkiThkz/#miizge=Lljq
_Hrje64('G-Tv-d0-
9%2H/%3U',kray/ymyrslkx)&drvlk=TDjMRK1LsGzIHo
vjNljAvZrhr3lUufNuKcdTHZ5YAdcZkgxbCNg0hY5ZYZ0
���
```

Base32 Decoder

Do not confuse with mathematical base 32 conversion!

➤ *Go to:* Base N Convert

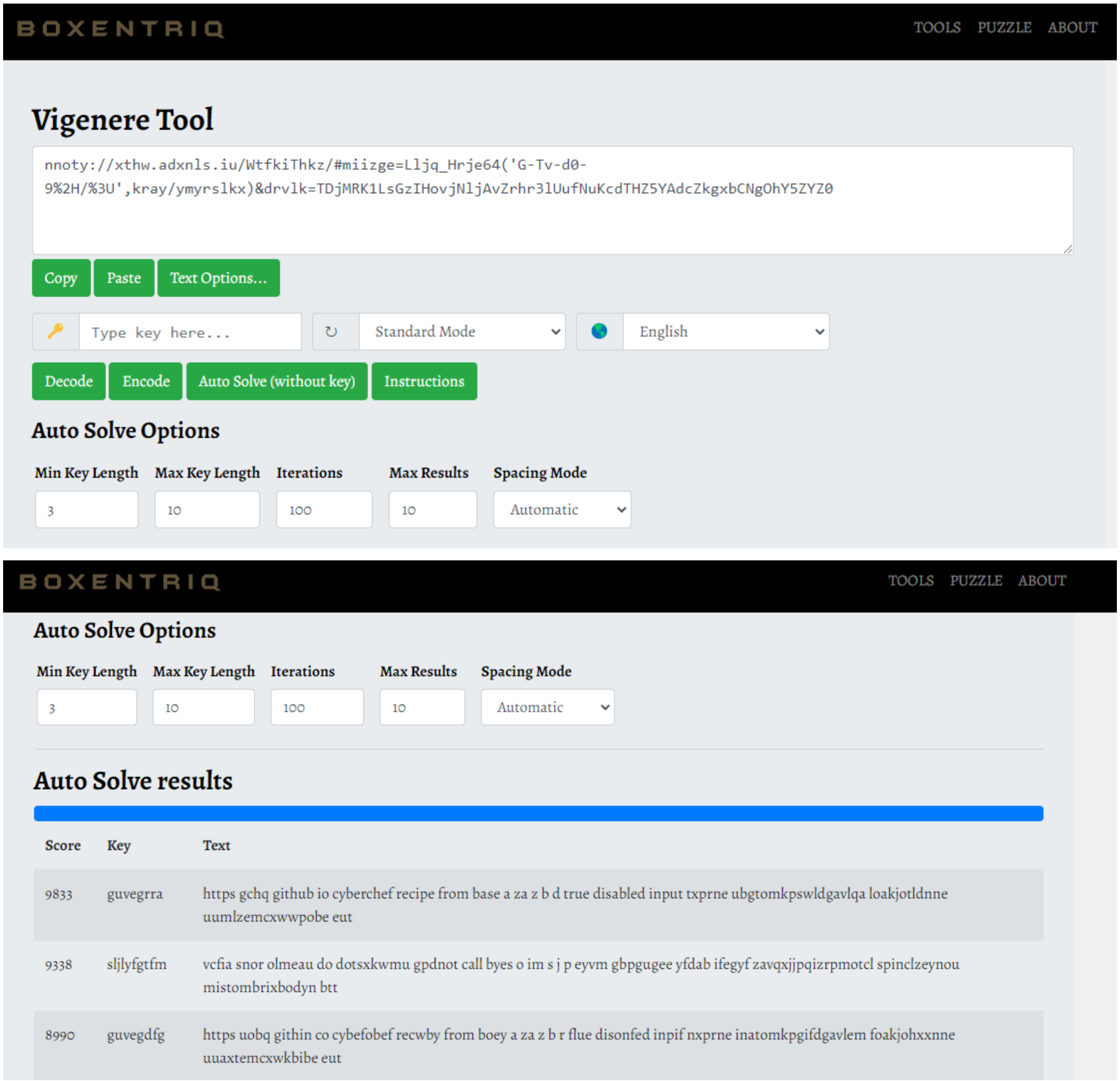
★ Base 32 ciphertext ?

```
NZXG65DZHIXS66DUNB3S4YLEPBXGY4ZONF2S6V3UMZVWSVDINN5C6I3NNFU
XUZ3FHVGGY2TRL5EHE2TFGY2CQJ2HFVKHMLLEGAWTSJJSJAXSKM2VE4WGW4
TBPEXXS3LZOJZWY23YFETGI4TWNRVT2VCENJGVESZRJRZUO6SJJBXXM2SON
RVEC5S2OJUHEM3MKV2WMTTVJNRWIVCILI2VSQLEMNNGWZ3YMJBU4Z2PNBMT
KWSZLIYA====
```

★ Results format ● ASCII (printable) characters
○ Hexadecimal 00-7F-FF
○ Decimal 0-127-255
○ Octal 000-177-377
○ Binary 00000000-11111111

We decided to continue investigating this case to figure out what type of link this was for. Fortunately, the cipher identifier listed it having similarities to Vigenere decryption [1]. Upon further research, we found a site that has an “auto-solving” function (not requiring a key) and helped us provide better accuracy with the link, though it was still a little hazy to input into the browser (Figure 4) [2].

Figure 4



Vigenere Tool

```
nnoty://xthw.adxnls.iu/WtfkiThkz/#miizge=Lljq_Hrje64('G-Tv-d0-
9%2H/%3U',kray/ymyrslkx)&drvlk=TDjMRK1LsGzIHovjNljAvZrhr3lUufNuKcdTHZ5YAdcZkgxbCNgOhY5ZYZ0
```

Auto Solve Options

Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	10	100	10	Automatic

Auto Solve Options

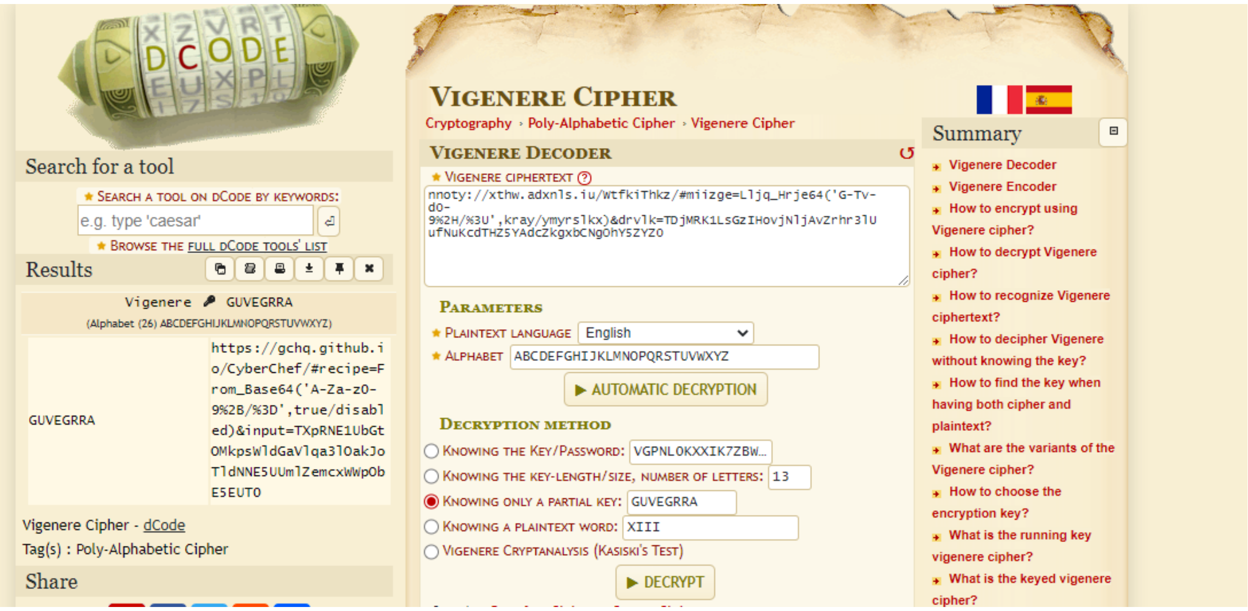
Min Key Length	Max Key Length	Iterations	Max Results	Spacing Mode
3	10	100	10	Automatic

Auto Solve results

Score	Key	Text
9833	guvegrra	https gchq github io cyberchef recipe from base a za z b d true disabled input txprne ubgtomkpswldgavlqa loakjotldnne uumlzemcxwwpobe eut
9338	sljlyfgtfm	vcfia snor olmeau do dotsxkwmu gpdnot call byes o im s j p eyvm gbpgugee yfdab ifegyf zavqxjjpqizrpmotcl spinclzeynou mistombrixbodyn btt
8990	guvegdfg	https uobq githin co cybefobef recwby from boey a za z b r flue disonfed inpif nxprne inatomkpgifdgavlem foakjohxxnne uuaxtemcxwkbibe eut

As noticed above, the link is almost there, giving us an idea of what we are now looking for. It is a github link that we are going to use. Some extra thinking led us to copying the key name that was generated for us by the site and inputting it in dCode's Vigenere Cipher, which can take "partial keys" as an option [2]. Hoping this would provide us with a better link that was better in nature due to case-sensitive characters in the URL, we decoded the string and ended up with a link that was easy to copy and paste into our browser (Figure 5).

Figure 5


Search for a tool
★ Search a tool on dCode by keywords:
e.g. type 'caesar'
★ Browse the full dCode tools' list
Results
Share
Vigenere Cipher
Cryptography › Poly-Alphabetic Cipher › Vigenere Cipher
Vigenere Decoder
Parameters
▶ AUTOMATIC DECRYPTION
Decryption method
▶ DECRYPT
Summary
Vigenere Decoder
Vigenere Encoder
How to encrypt using Vigenere cipher?
How to decrypt Vigenere cipher?
How to recognize Vigenere ciphertext?
How to decipher Vigenere without knowing the key?
How to find the key when having both cipher and plaintext?
What are the variants of the Vigenere cipher?
How to choose the encryption key?
What is the running key vigenere cipher?
What is the keyed vigenere cipher?

★ Vigenere ciphertext

```
nnoty://xthw.adxnls.iu/WtfkiThkz/#miizge=Lljq_Hrje64('G-Tv-
dO-
9%2H/%3U',kray/ymyrslkx)&drvlk=TDjMRK1LsGzIHovjNljAvZrhr3lU
ufNuKcdTHZ5YAdcZkgxbCNgOhY5ZYZO
```

★ Plaintext language: English

★ Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ

○ Knowing the Key/Password: VGPNLOKXXIK7ZBW...

○ Knowing the key-length/size, number of letters: 13

● Knowing only a partial key: GUVEGRRA

○ Knowing a plaintext word: XIII

○ Vigenere Cryptanalysis (Kasiski's Test)

Vigenere 🔑 GUVEGRRA

(Alphabet (26) ABCDEFGHIJKLMNOPQRSTUVWXYZ)

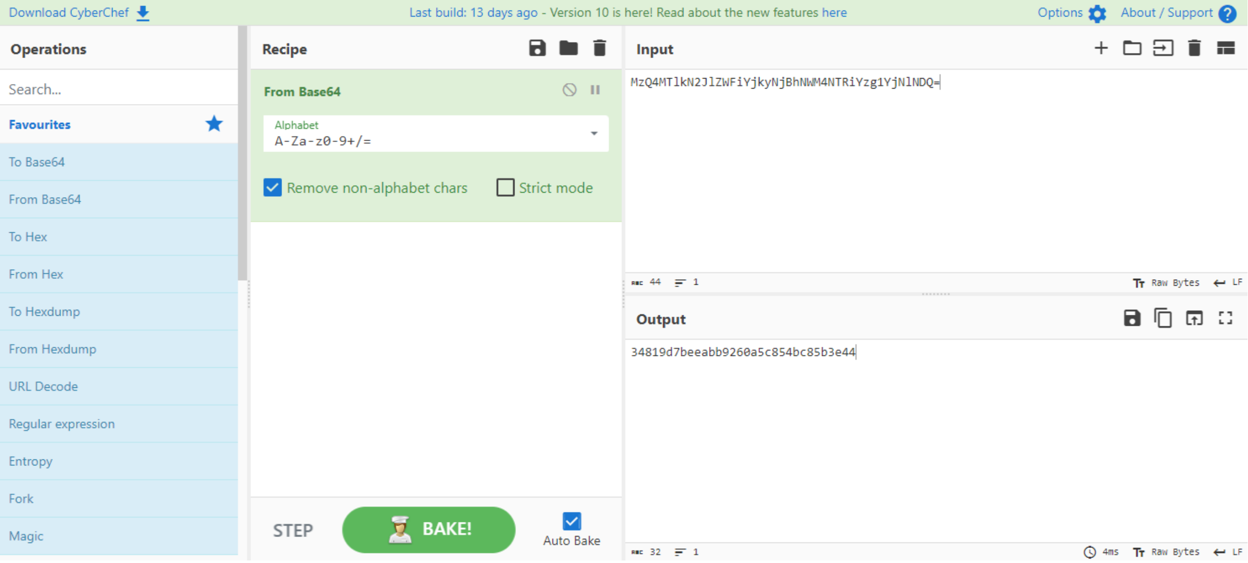
GUVEGRRA	https://gchq.github.io/CyberChef/#recipe=From_Base64('A-Za-z0-9%2B/%3D',true/disabled)&input=TXpRNE1UbGtOMkpsWldGaVlqa3lOakJoTldNNE5UUmlZemcxWWpObE5EUT0

Vigenere Cipher - dCode

Tag(s) : Poly-Alphabetic Cipher

Pasting this link into Chrome, we arrive on a site which originally had the same input and output. By clicking the “Disable” button next to the “Pause” button, this changed the output of the text [3]. It appears to be an MD5 hash (Figure 6).

Figure 6



From Base64

Alphabet: A-Za-z0-9+/=

☑ Remove non-alphabet chars ☐ Strict mode

Input

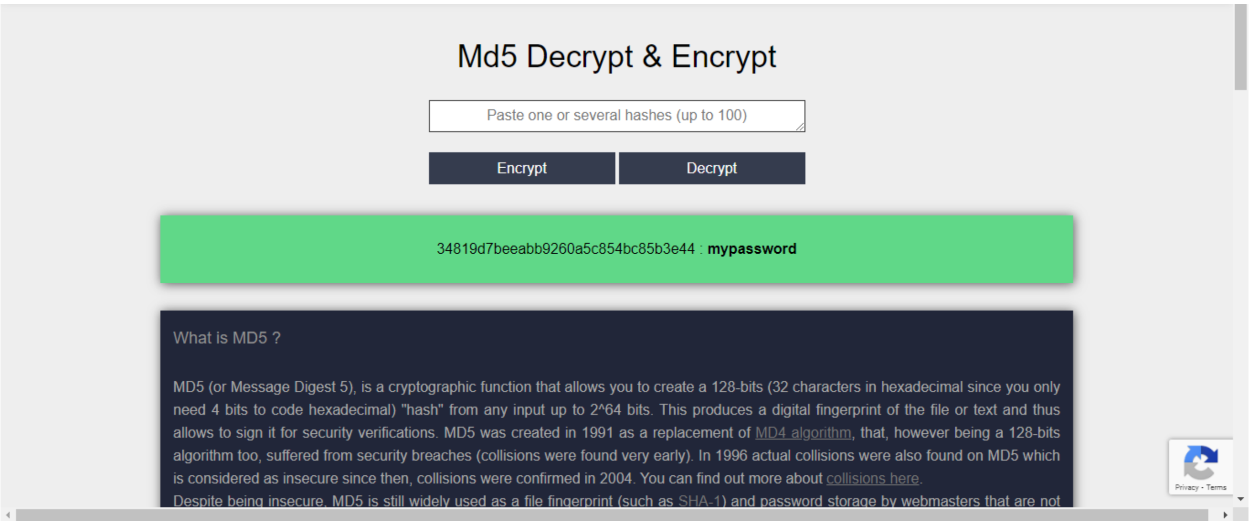
```
MzQ4MTlkN2JlZWFiYjkyNjBhNWM4NTRiYzg1YjNlNDQ=
```

Output

```
34819d7beeabb9260a5c854bc85b3e44
```

Upon putting in the MD5 hash into a decryption service, it came out that the hash is “mypassword” (Figure 7) [4]. Therefore, we believe that “mypassword” is the password.

Figure 7



Md5 Decrypt & Encrypt

34819d7beeabb9260a5c854bc85b3e44 : **mypassword**

What is MD5 ?

MD5 (or Message Digest 5), is a cryptographic function that allows you to create a 128-bits (32 characters in hexadecimal since you only need 4 bits to code hexadecimal) "hash" from any input up to 2^64 bits. This produces a digital fingerprint of the file or text and thus allows to sign it for security verifications. MD5 was created in 1991 as a replacement of MD4 algorithm, that, however being a 128-bits algorithm too, suffered from security breaches (collisions were found very early). In 1996 actual collisions were also found on MD5 which is considered as insecure since then, collisions were confirmed in 2004. You can find out more about collisions here.
Despite being insecure, MD5 is still widely used as a file fingerprint (such as SHA-1) and password storage by webmasters that are not

References

[1] dCode, "dCode," dCode, 2023. [Online]. Available: https://www.dcode.fr/. [Accessed April 2023].

[2] J. Ahlen, "Vigenere Cipher," Boxentriq, 2023. [Online]. Available: https://www.boxentriq.com/code-breaking/vigenere-cipher. [Accessed April 2023].

[3] Crown, "CyberChef," Crown Copyright, 2016. [Online]. Available: https://gchq.github.io/CyberChef/. [Accessed April 2023].

[4] Md5Decrypt.net, "Md5 Decrypt & Encrypt," Md5Decrypt, 2022. [Online]. Available: https://md5decrypt.net/en/. [Accessed April 2023].