HackerFrogs Afterschool
Classical Ciphers (Part 1)

Class:
Cryptography

Workshop Number:
AS-CRY-02

Document Version:
1.75

Special Requirements:
Registered account at
picoctf.org

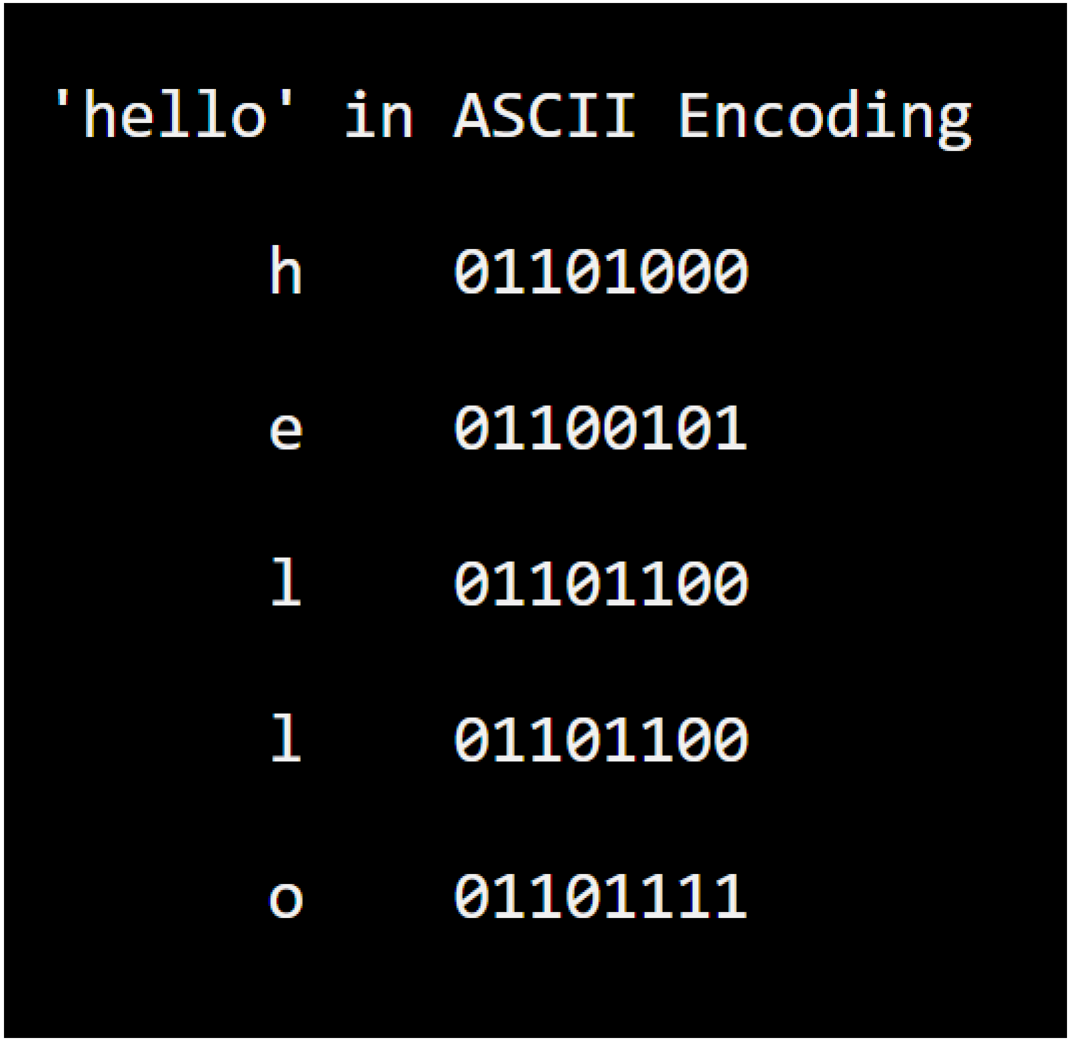
Welcome to HackerFrogs Afterschool!

Hey there HackerFrogs! This workshop is the second session for cryptography basics

In the last session we learned about the following cryptography concepts

Encoding

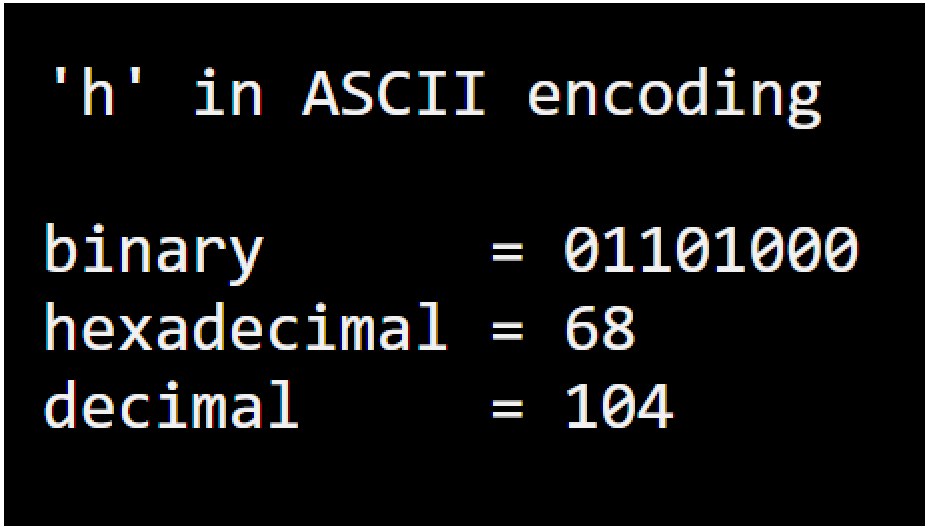
Encoding refers to the process of converting data from one form to another, often for the purpose of efficient storage, transmission, or representation.



```
'hello' in ASCII Encoding

      h    01101000

      e    01100101

      l    01101100

      l    01101100

      o    01101111
```

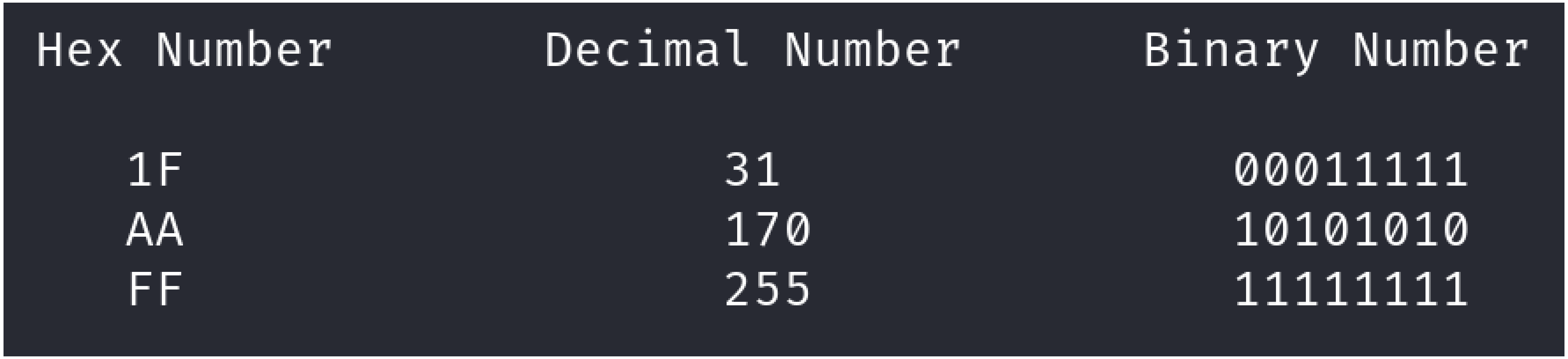
ASCII Encoding

ASCII is a common text encoding system which assigns numerical values to letters, numbers, and symbols



```
'h' in ASCII encoding

binary      = 01101000
hexadecimal = 68
decimal     = 104
```

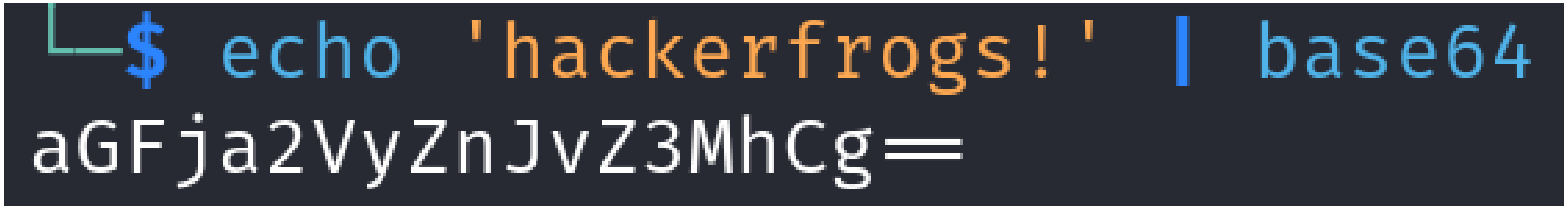
Hexadecimal Conversion



Hex Number	Decimal Number	Binary Number
1F	31	00011111
AA	170	10101010
FF	255	11111111

Hexadecimal can be used to represent ASCII characters, and conversion between hex and ASCII is a form of encoding

Base64 Encoding



```
└─$ echo 'hackerfrogs!' | base64
aGFja2VyZnJvZ3MhCg==
```

Base64 is a method of converting data bytes into alphanumeric strings, and is often featured in CTF challenges

Encoding is not Encryption

Although encoding transforms data from one form to another, the intention of encoding is not to hide the contents of the data, so it is not cryptography

Encoding is not Encryption

Additionally, encoding methods are meant to be well-known and easily-reversible, which further sets encoding apart from encryption

This Session's Topics

- Cryptography Terminology

- Classical Ciphers

- ROT13 Cipher

- Caesar Cipher

What is Cryptography?

Let's start our exploration of cryptography by going over some key terms.

Intro to Cryptography Terms

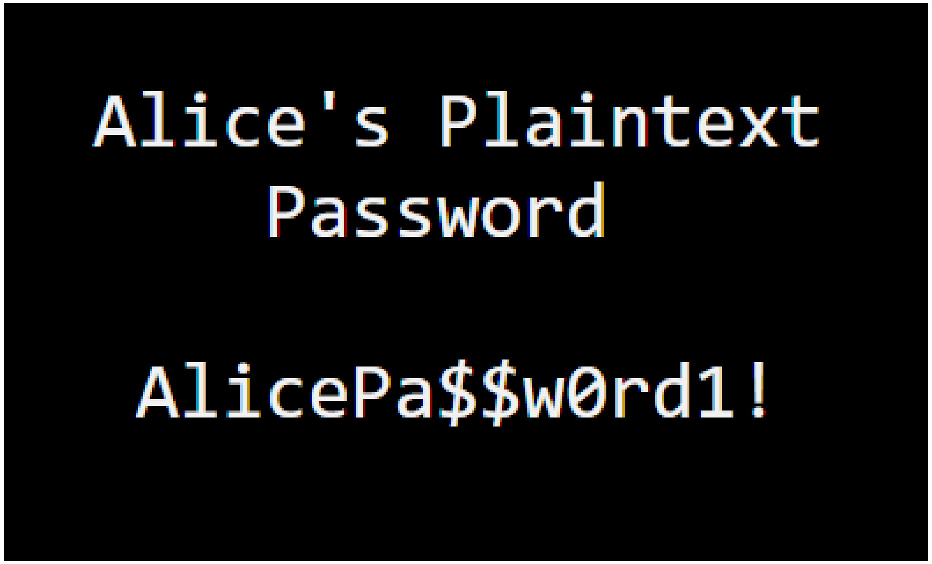
Let's suppose that Bob wants to use Alice's streaming video app account to watch some movies.

Intro to Cryptography Terms

Alice is fine with Bob using her account, but wants to send her account password to Bob secretly, to which Bob agrees.

Plaintext / Cleartext

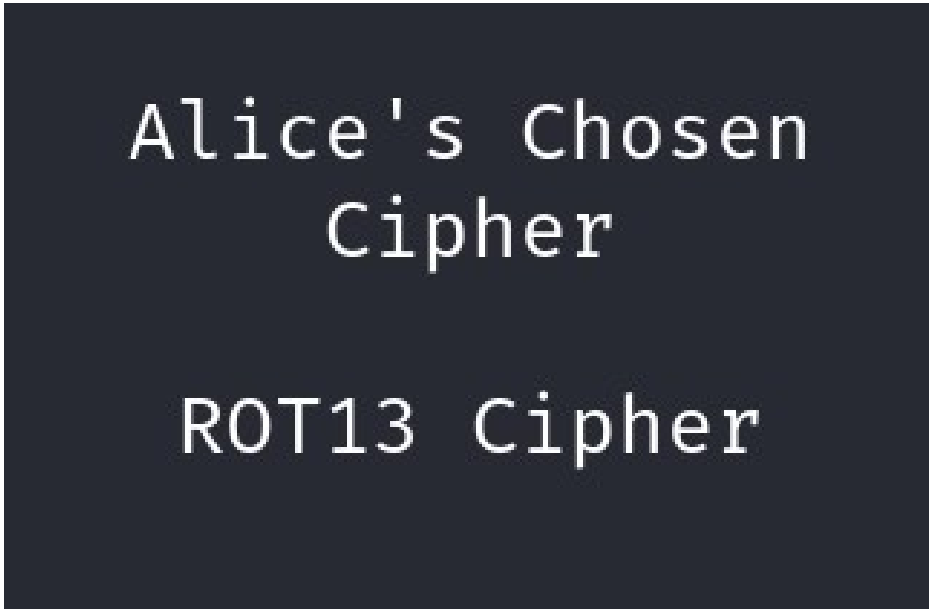
Alice's password before it is transformed into a secret message through cryptography, is called **plaintext** or **cleartext**.



```
Alice's Plaintext
    Password

 AlicePa$$w0rd1!
```

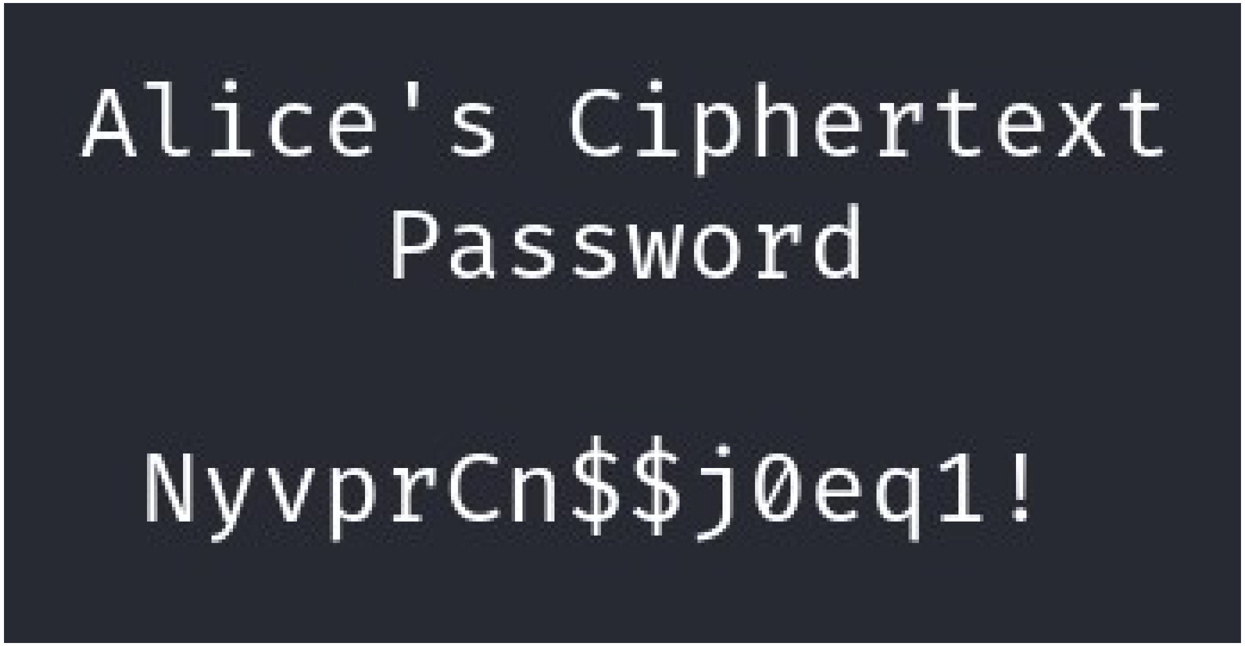
Ciphers

Alice then uses a cryptographic algorithm called a **cipher** to transform the message from its original form into a secret message.



```
Alice's Chosen
    Cipher

 ROT13 Cipher
```

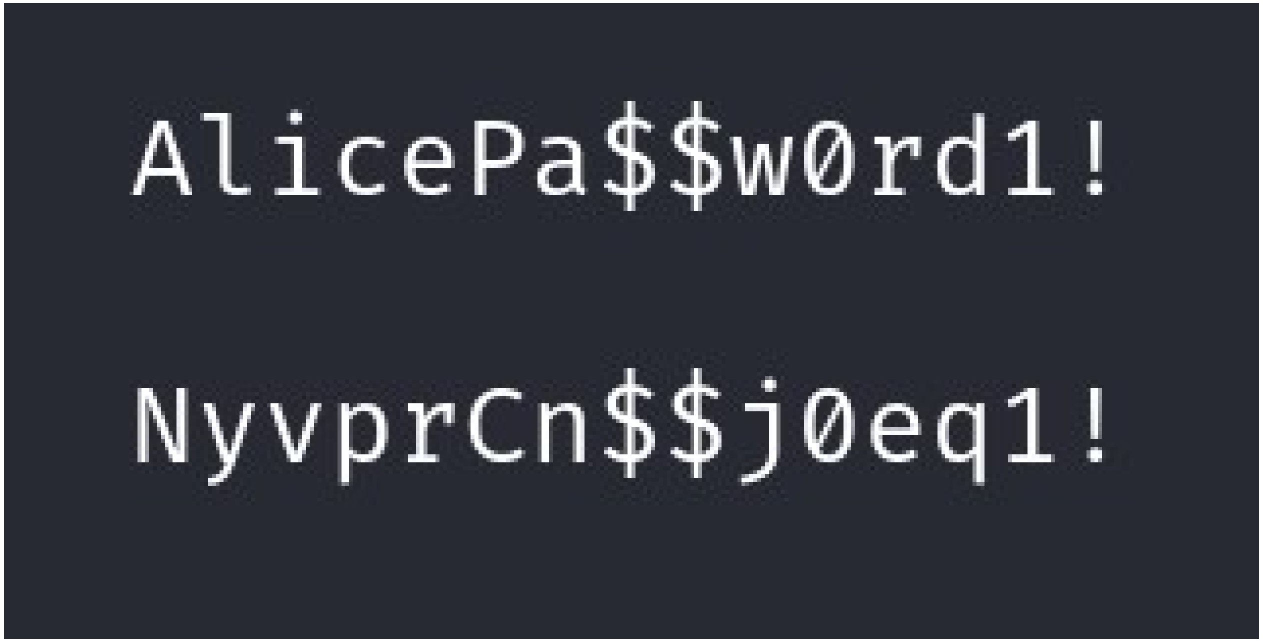
Ciphertext



```
Alice's Ciphertext
     Password

  NyvprCn$$j0eq1!
```

This secret form of the message is called **ciphertext**.

Encryption



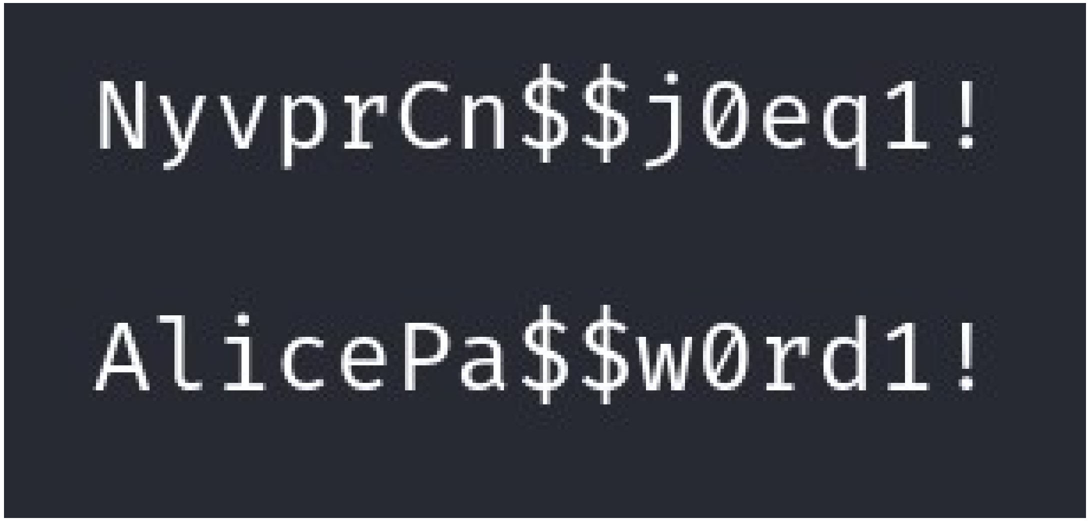
```
AlicePa$$w0rd1!

NyvprCn$$j0eq1!
```

The act of transforming plaintext into ciphertext is called **encryption**.

Intro to Cryptography Terms

Alice then sends the message with the encrypted password to Bob, and tells him which cipher was used to encrypt the password

Intro to Cryptography Terms



```
NyvprCn$$j0eq1!

AlicePa$$w0rd1!
```

Upon receiving the message, Bob uses the same cipher to transform the ciphertext back into plaintext. This act is called **decryption**.

Intro to Cryptography Terms

After decrypting the message from Alice, Bob can use the password to log into Alice's streaming video app account and watch movies.

Intro Cryptography Terms

Cipher - A cryptographic algorithm used in encryption and decryption

Plaintext - A message or piece of text that is not encrypted

Ciphertext - An encrypted message or piece of text

Encryption - The act of transforming plaintext into ciphertext

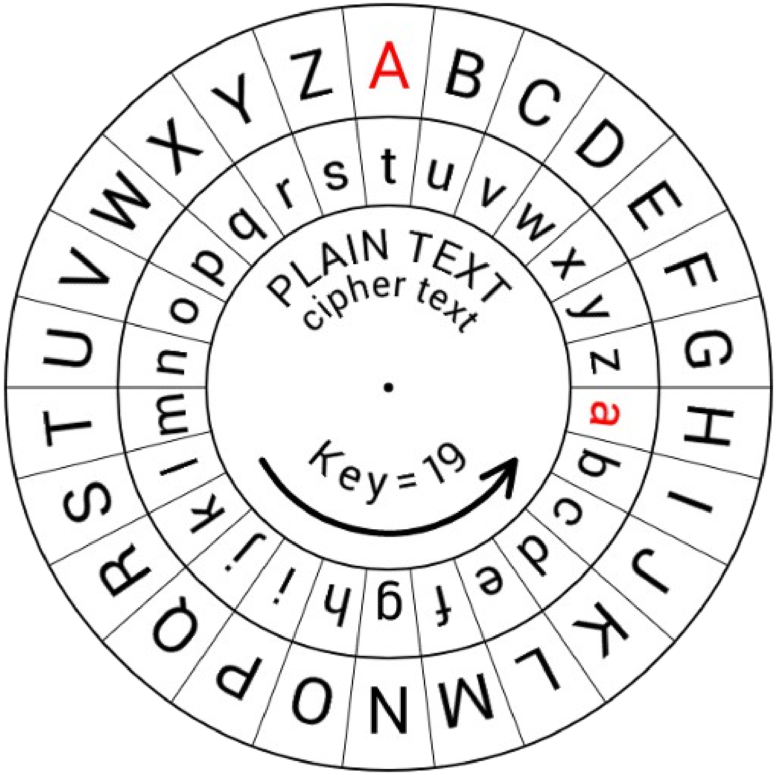
Decryption - The act of transforming ciphertext into plaintext

Classical Ciphers and Modern Cryptographic Ciphers

Cryptography ciphers can be divided into two categories: **classical ciphers** and **modern ciphers**

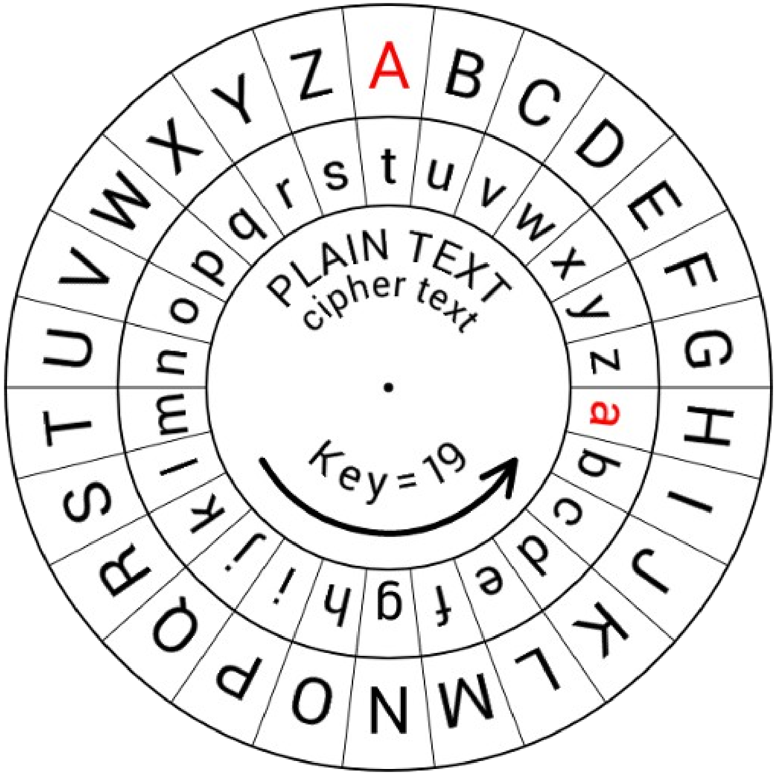
Classical Ciphers and Modern Cryptographic Ciphers

Classical ciphers refer to cryptographic ciphers used prior to the introduction of computer-aided algorithms


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key = 19

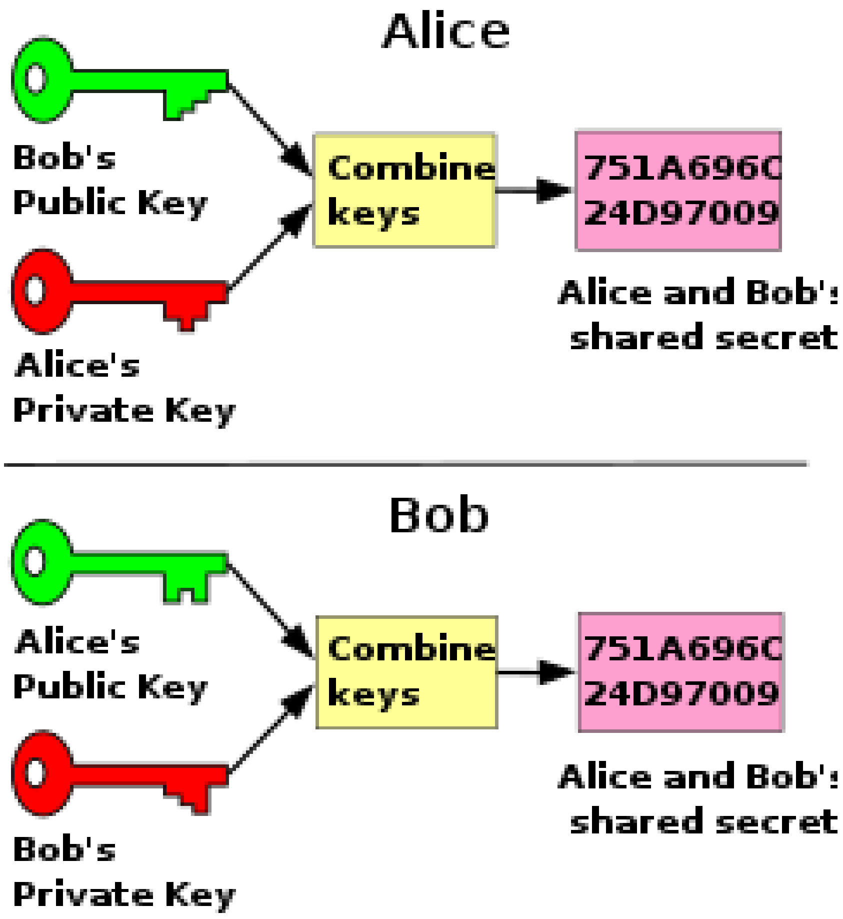
Classical Ciphers and Modern Cryptographic Ciphers

With classical ciphers, it is generally possible to perform the steps required to encrypt and decrypt messages without the aid of computers or calculators


PLAIN TEXT
cipher text
Key = 19
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
a b c d e f g h i j k l m n o p q r s t u v w x y z

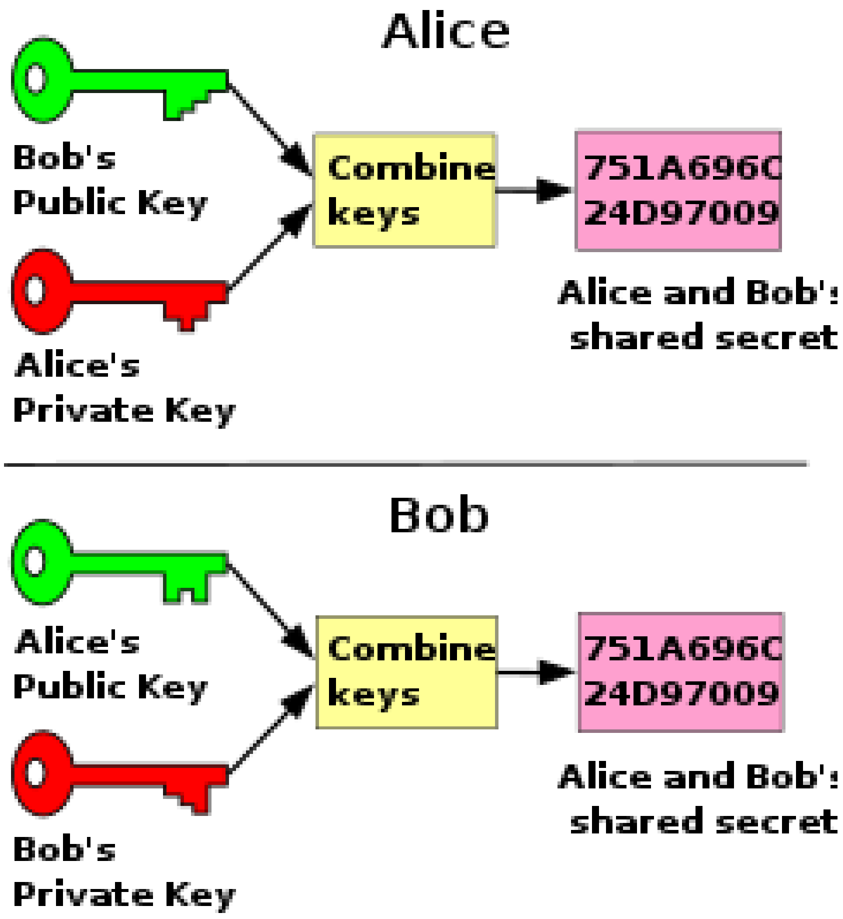
Classical Ciphers and Modern Cryptographic Ciphers

Modern ciphers are ciphers that incorporate complex mathematical operations in their encryption / decryption processes, and are impractical to use without the aid of computer processing



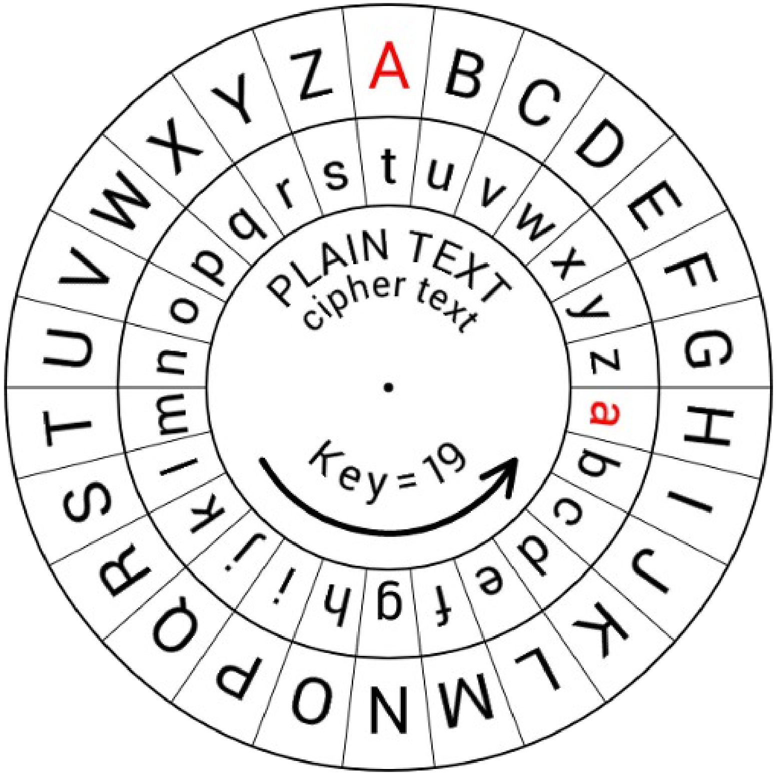
Classical Ciphers and Modern Cryptographic Ciphers

Virtually all ciphers used in computer security fall under this category



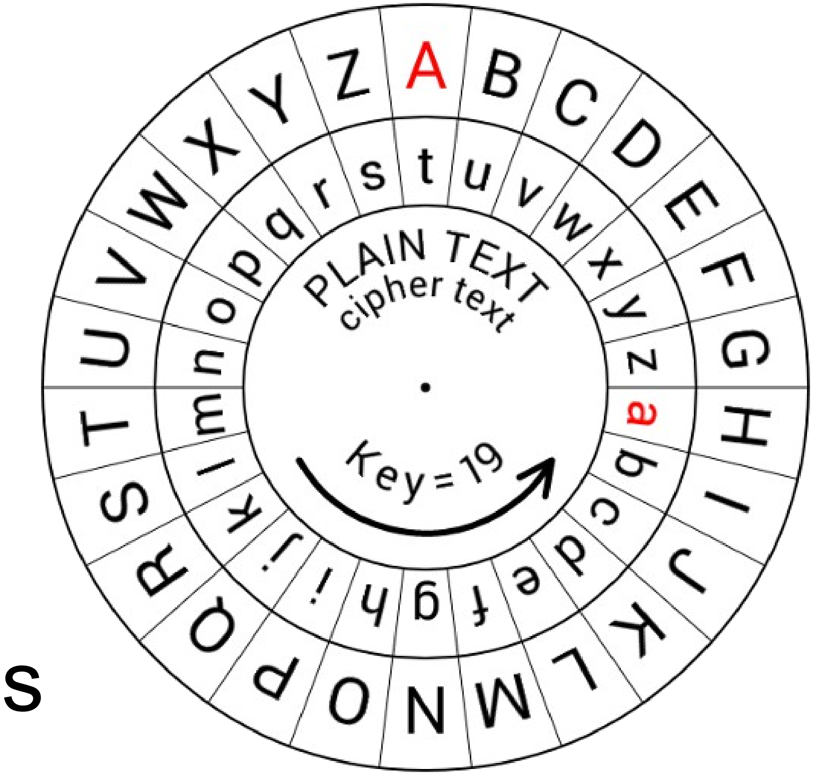
Classical Ciphers and Modern Cryptographic Ciphers

In our introduction to cryptography, we will first learn about classical ciphers for the following two reasons:


A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s
PLAIN TEXT
cipher text
Key = 19

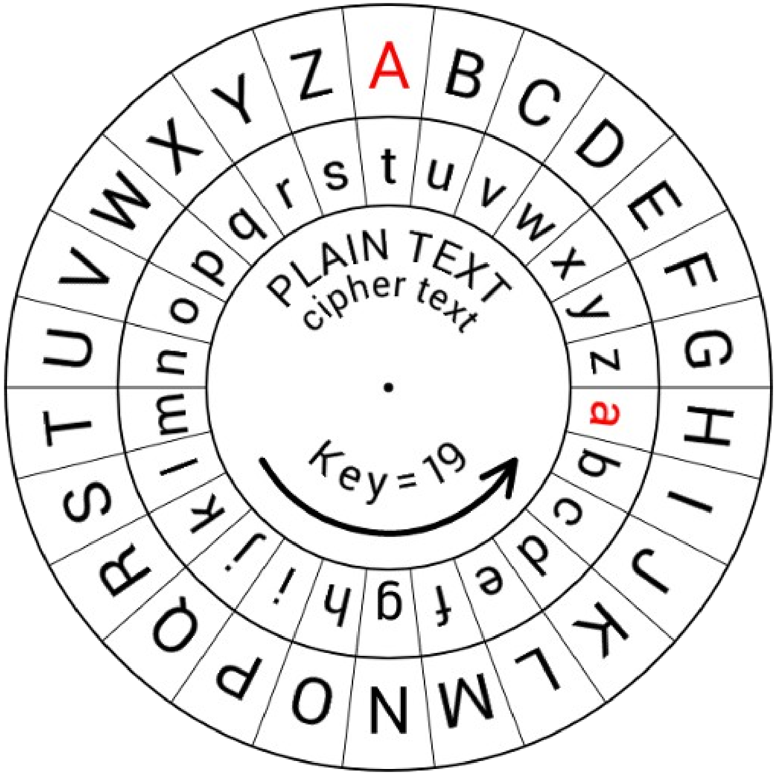
Classical Ciphers and Modern Cryptographic Ciphers

1) Beginner cryptography CTF exercises cover classical ciphers extensively, so we need to learn classical ciphers in order to engage with and solve those challenges



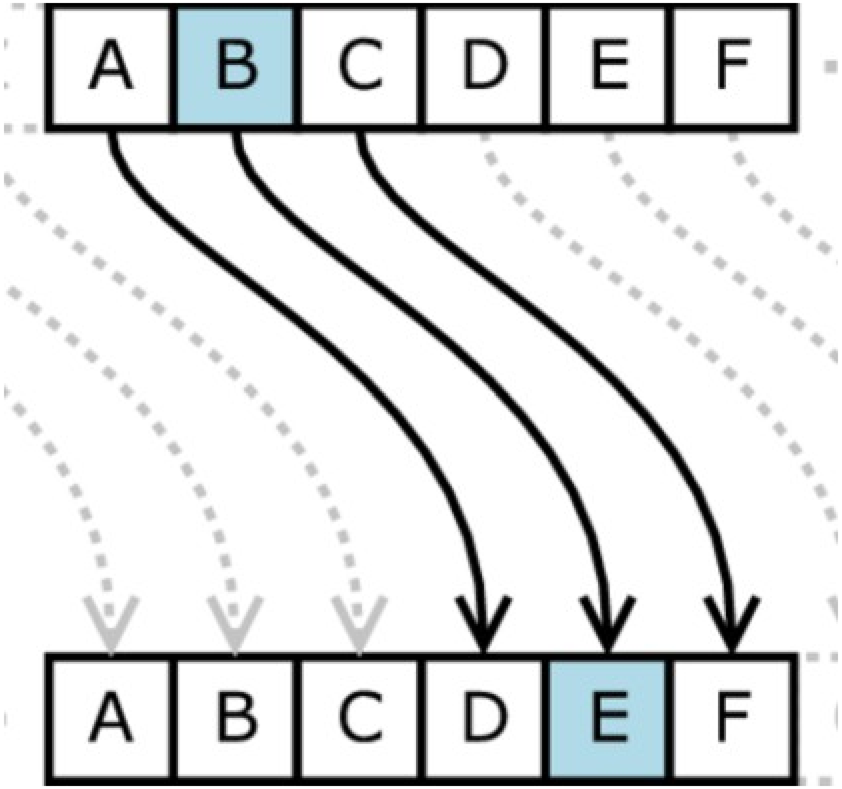
Classical Ciphers and Modern Cryptographic Ciphers

2) More importantly, as an introduction to cryptography, the methods involved in classical cryptography are much easier to understand, since they do not require complex mathematical operations


PLAIN TEXT
cipher text
Key = 19
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
t u v w x y z a b c d e f g h i j k l m n o p q r s

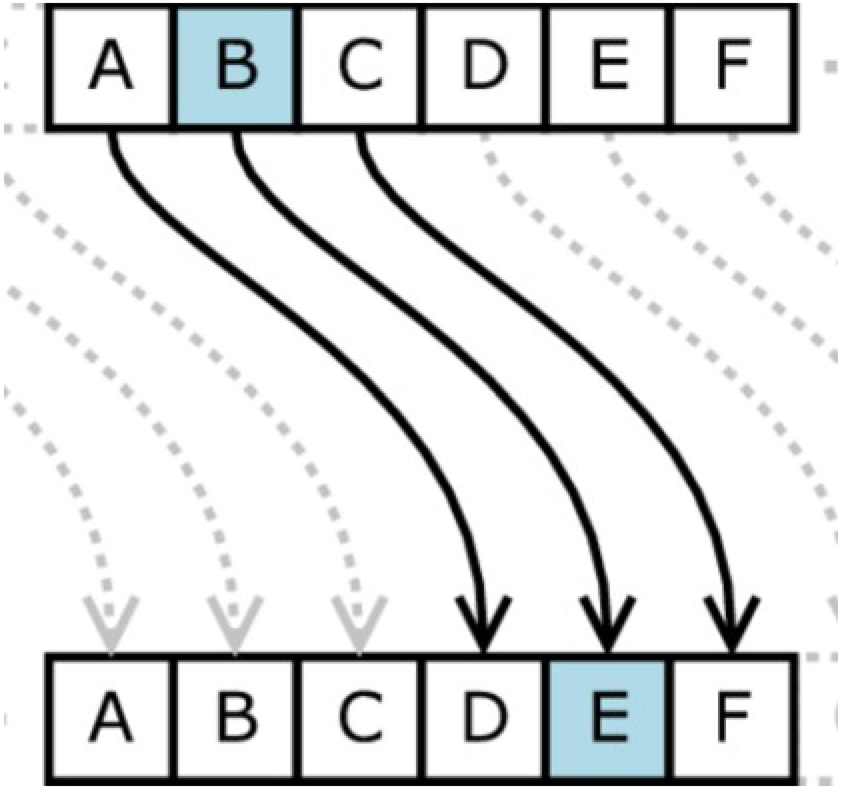
Substitution Ciphers

Substitution ciphers are a type of classical cryptographic cipher where one portion of the plaintext is substituted for a portion of ciphertext during encryption.

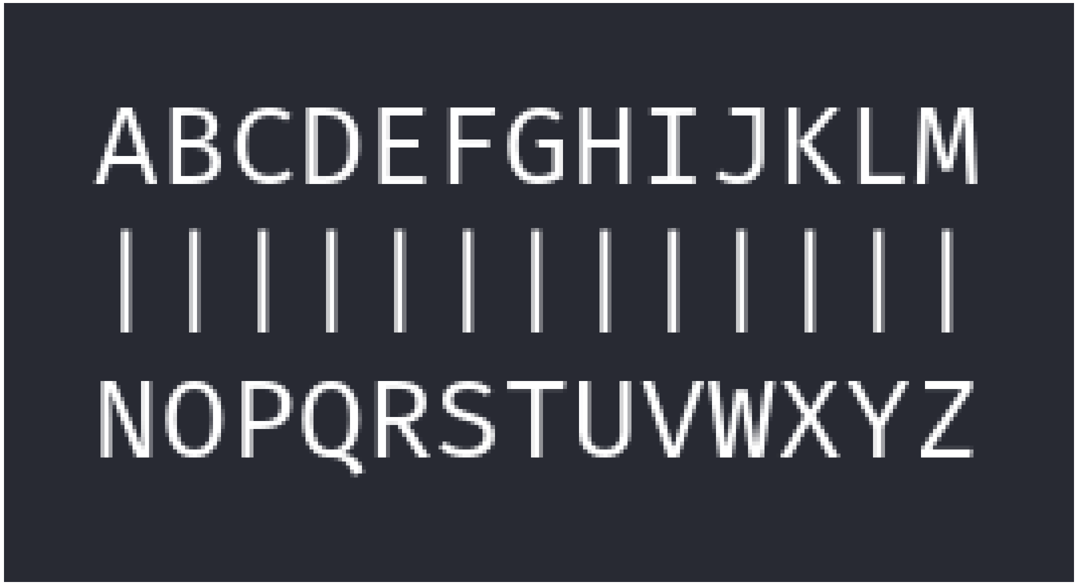


Substitution Ciphers

The size of the portions may be symmetrical (e.g., one character of plaintext is substituted by one character of ciphertext) or asymmetrical (e.g., one character of plaintext is substituted by two characters of ciphertext or vice versa).



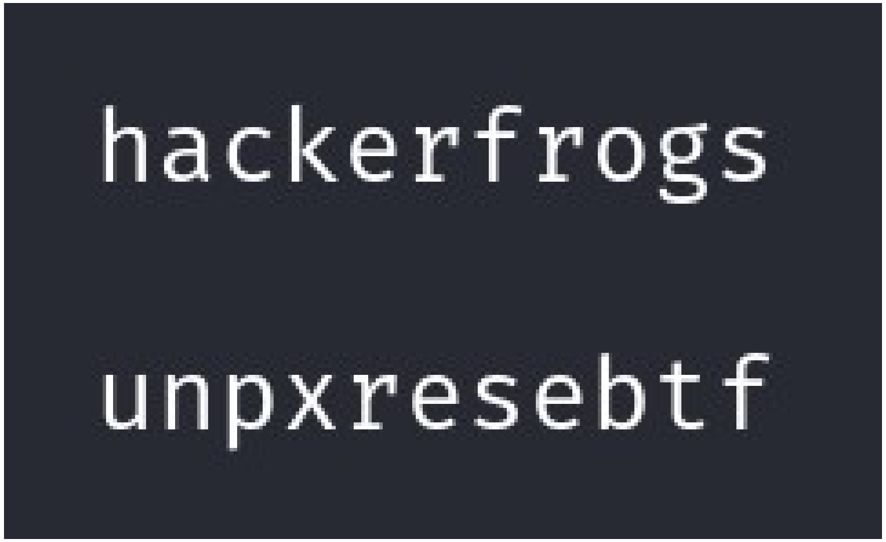
ROT13 Cipher



```
ABCDEFGHIJKLM
|||||||||||||
NOPQRSTUVWXYZ
```

The ROT13 cipher is a simple substitution cipher where the encryption method is shift each plaintext letter 13 positions in the alphabet to form the ciphertext

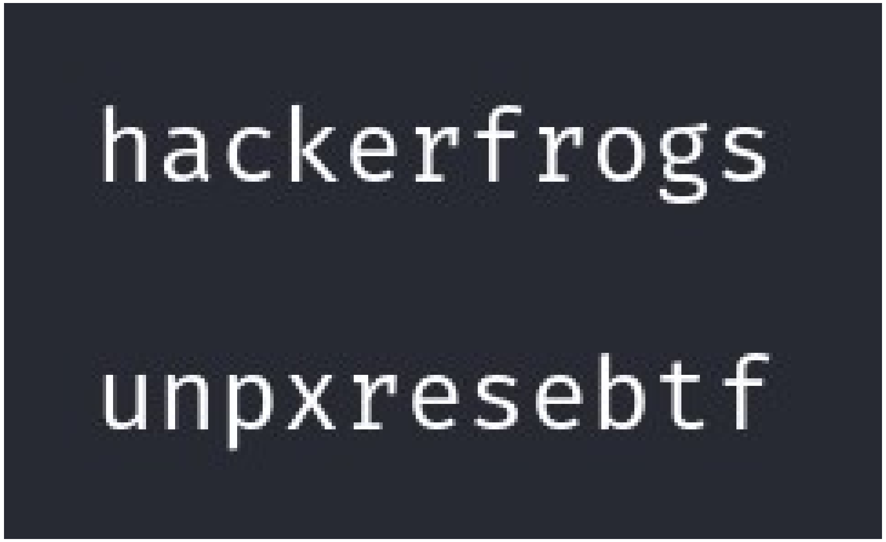
ROT13 Cipher



```
hackerfrogs

unpxresebtf
```

So if we use this cipher to encrypt the plaintext `hackerfrogs`, the resulting ciphertext would be `unpxresebtf`

ROT13 Cipher



```
hackerfrogs

unpxresebtf
```

To decrypt the ciphertext we would do the same operation, shifting each ciphertext letter by 13 places in the alphabet

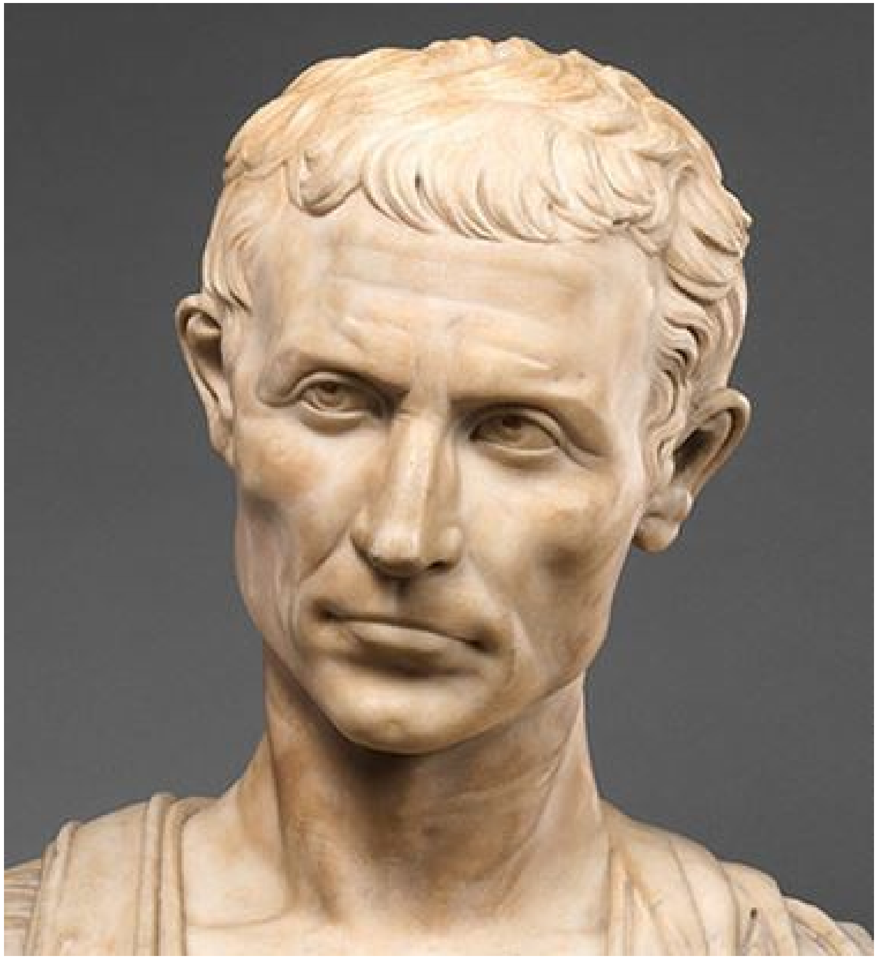
PicoCTF - 13

Let's learn more about the ROT13 cipher by working through a challenge on PicoCTF. Navigate to the following URL

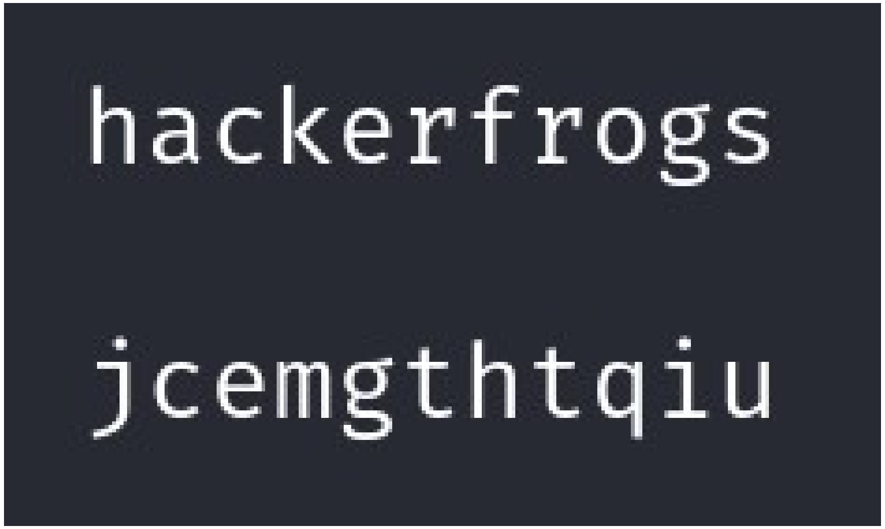
https://play.picoctf.org/practice/challenge/62?category=2&page=1

The Caesar Cipher

The Caesar Cipher is a substitution cipher where the method of encryption is to shift each letter of the plaintext by a specific number of letters in the alphabet, called the shift or key



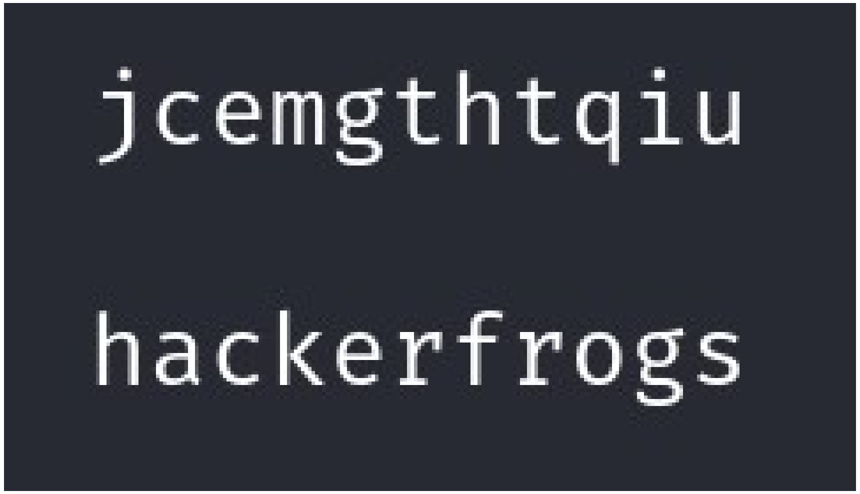
The Caesar Cipher



```
hackerfrogs

jcemgthtqiu
```

For example, if we use the Caesar cipher with a shift of 2 to encrypt the plaintext `hackerfrogs`, we would shift each letter two positions in the alphabet, and the resulting ciphertext would be `jcemgthtqiu`

The Caesar Cipher



```
jcemgthtqiu

hackerfrogs
```

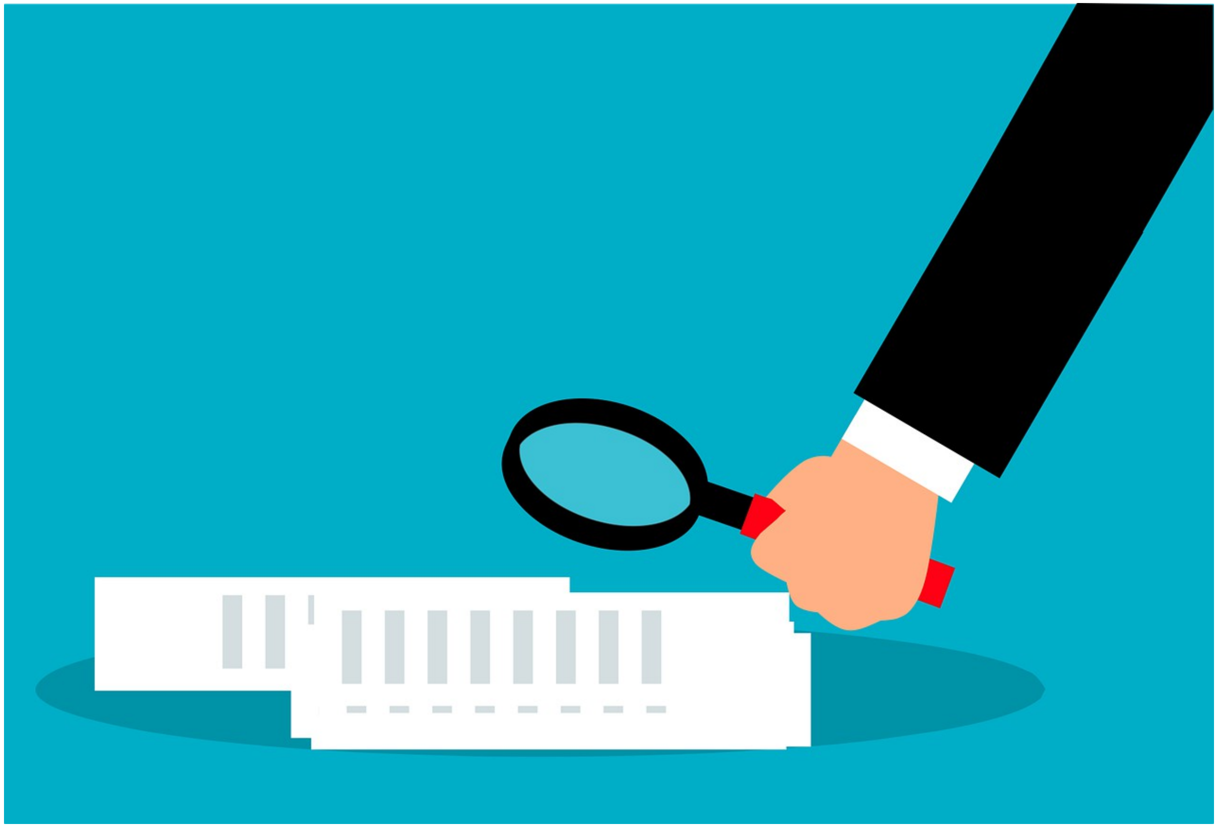
To decrypt the ciphertext, we take each letter of it, and shift back two letters in the alphabet to form the plaintext

PicoCTF - Rotation

Let's learn more about Caesar cipher by working through a challenge on PicoCTF. Navigate to the following URL

https://play.picoctf.org/practice/challenge/373?category=2&page=1

Summary



Let's review the cryptography concepts we learned in this workshop:

Cryptography Terms

`Cipher` - **A cryptographic algorithm used in encryption and decryption**

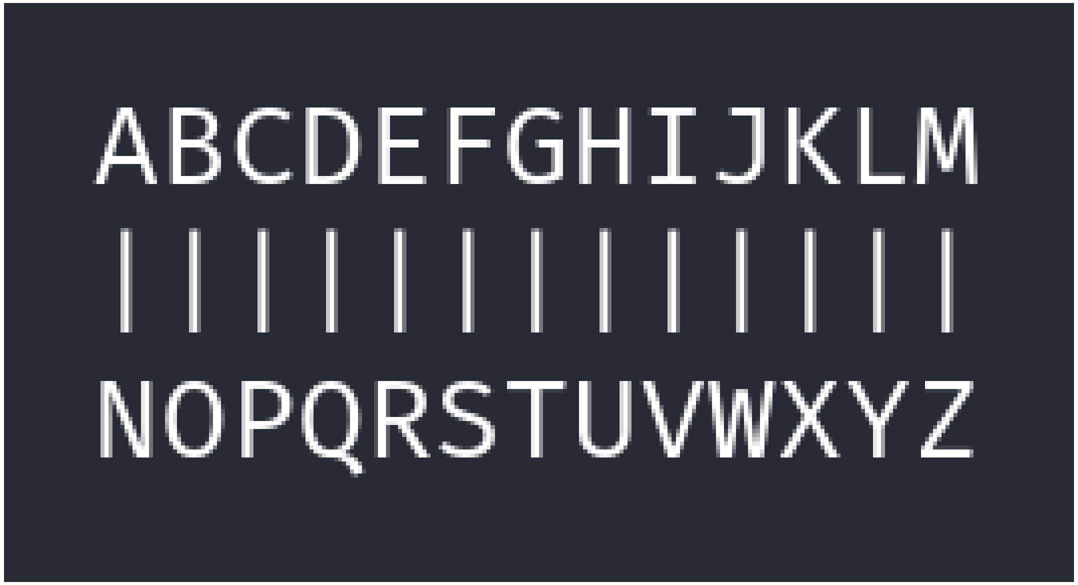
`Plaintext` - **A message or piece of text that is not encrypted**

`Ciphertext` - **An encrypted message or piece of text**

`Encryption` - **The act of transforming plaintext into ciphertext**

`Decryption` - **The act of transforming ciphertext into plaintext**

ROT13 Cipher

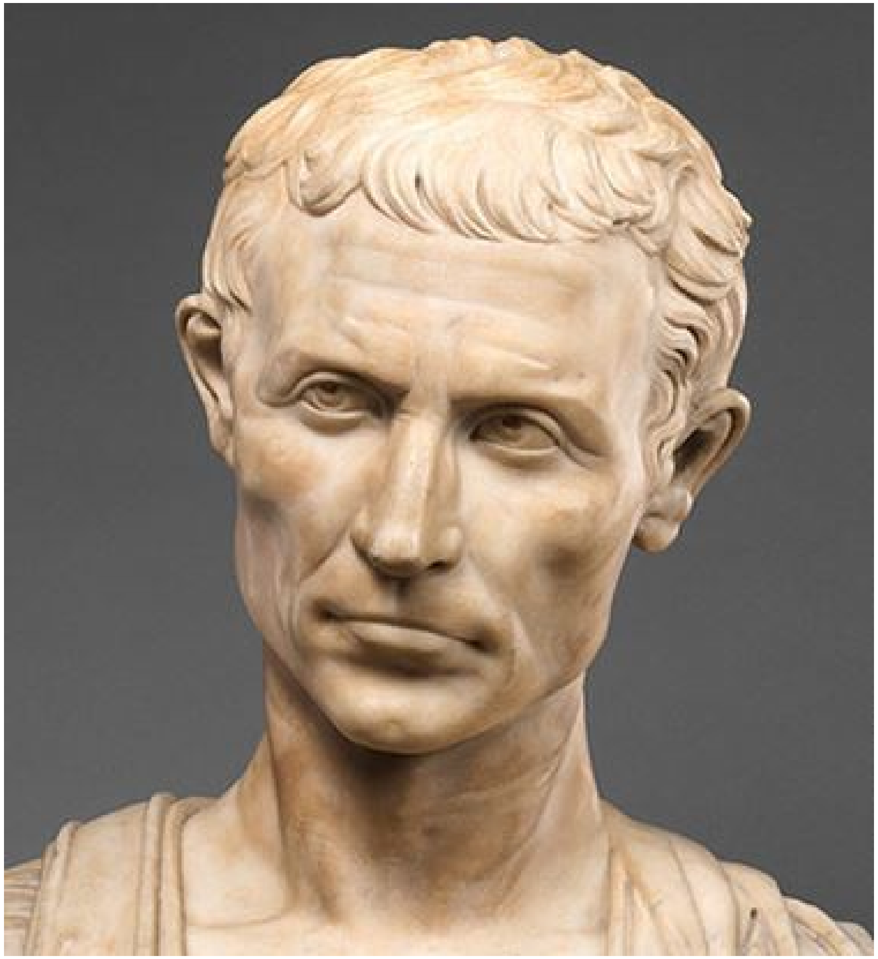


```
ABCDEFGHIJKLM
|||||||||||||
NOPQRSTUVWXYZ
```

The ROT13 cipher is a simple substitution cipher where the encryption method is shift each plaintext letter 13 positions in the alphabet to form the ciphertext

The Caesar Cipher

The Caesar Cipher is a substitution cipher where the method of encryption is to shift each letter of the plaintext by a specific number of letters in the alphabet, called the shift or key



What's Next?

In the next HackerFrogs Afterschool Cryptography workshop, we'll take another look at classical ciphers with more commonly-used ciphers, such as the Vigenere cipher

Until Next Time, HackerFrogs!