S.H.E.L.L.

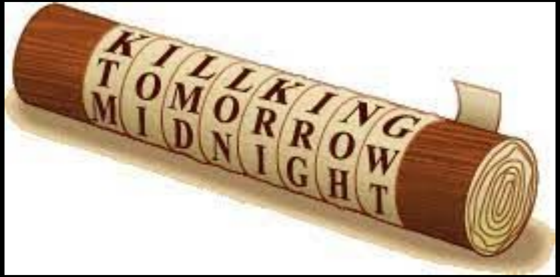
SECURITY IS AN ILLUSION

Cryptography

Historical Background

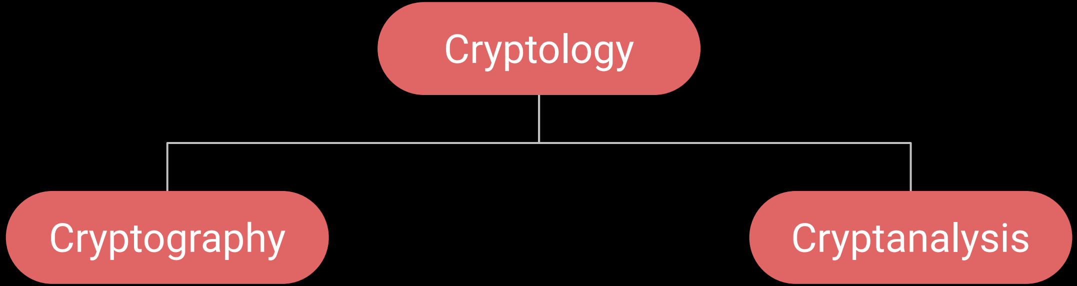
DECIDES TO DOCUMENT THE HISTORY OF CRYPTO
USES A BUNCH OF MEMES INSTEAD

Hieroglyphics cipher



Scytale of Sparta

Cryptology

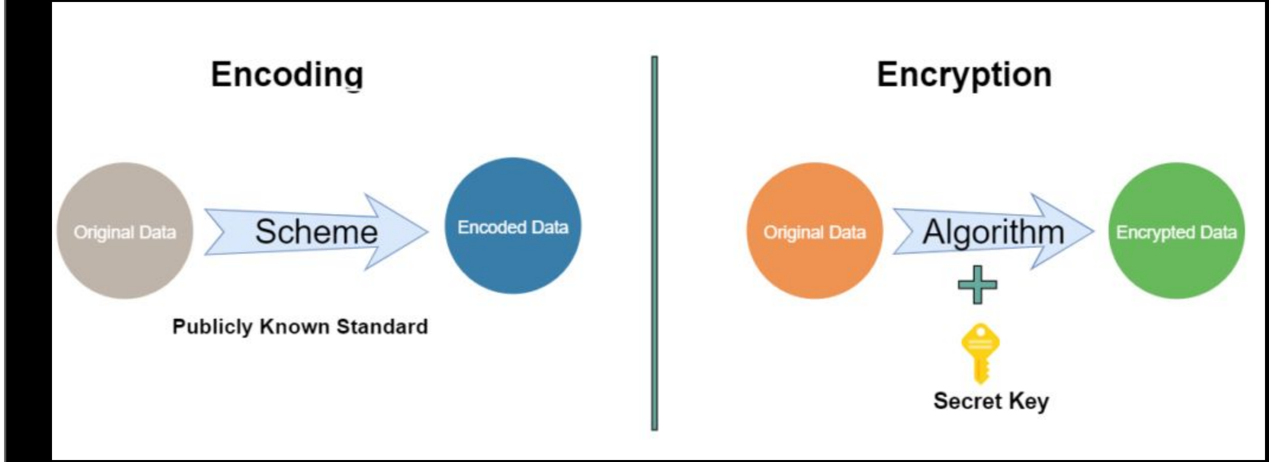


Cryptology

Cryptography

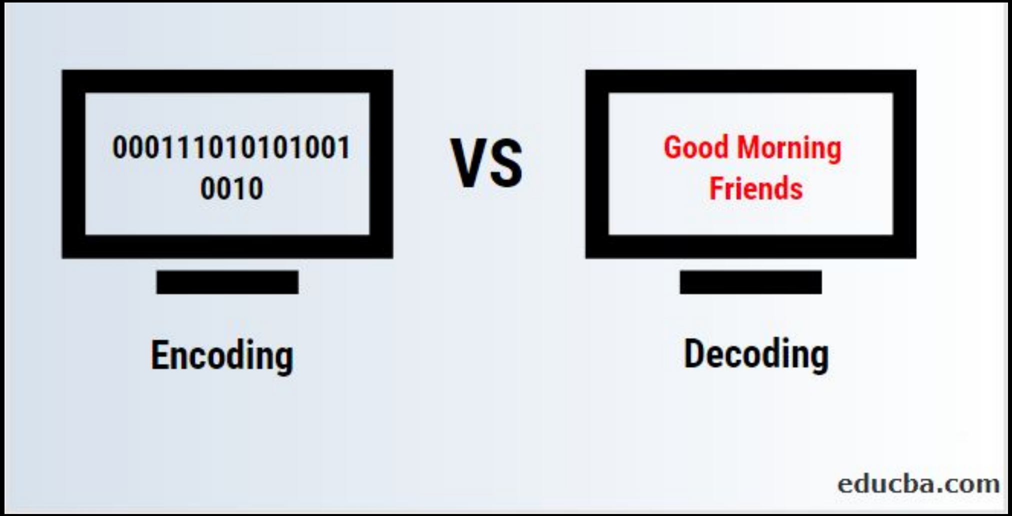
Cryptanalysis

Encryption & Encoding



Encoding

Using Base64 as “encryption”:



S.H.E.L.L.
SECURITY IS AN ILLUSION

Encoding

In the computing industry, standards are established to facilitate information interchanges among American coders. Unfortunately, I've made communication a little bit more difficult. Can you figure this one out? 41 42 43 54 46 7B 34 35 43 31 31 5F 31 35 5F 55 35 33 46 55 4C 7D

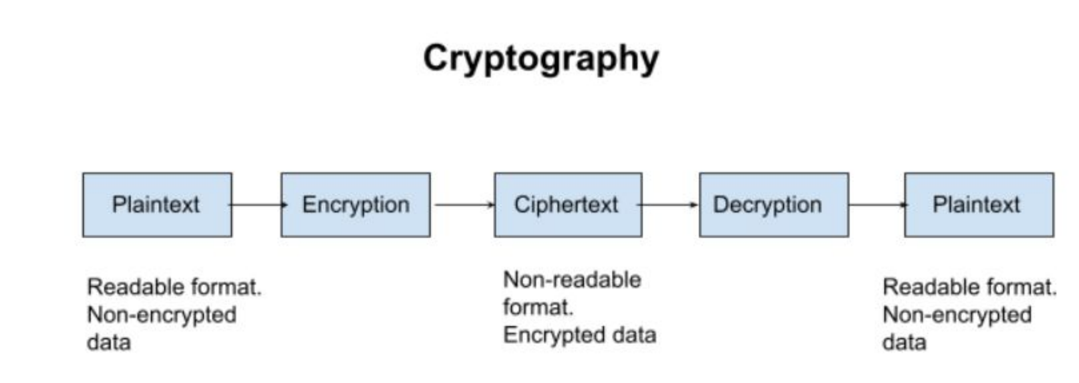
Challenge-1

When we encrypt something the resulting ciphertext commonly has bytes which are not printable ASCII characters. If we want to share our encrypted data, it's common to encode it into something more user-friendly and portable across different systems.

Included below is a flag encoded as a hex string. Decode this back into bytes to get the flag.

```
63727970746f7b596f755f77696c6c5f62655f776f7
26b696e675f776974685f6865785f737472696e67
735f615f6c6f747d
```

Encryption



Cryptography

Plaintext → Encryption → Ciphertext → Decryption → Plaintext

Plaintext: Readable format. Non-encrypted data

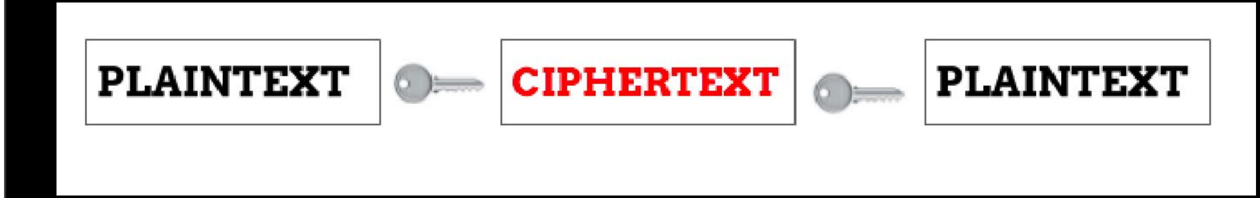
Ciphertext: Non-readable format. Encrypted data

Plaintext: Readable format. Non-encrypted data

Symmetric

- The same key is used to encrypt and decrypt, hence 'symmetric'.
- They key needs to be hidden and only given to receiver.
- Much faster, hence better for large data.
- Ex: Caesar cipher, XOR, DES, AES

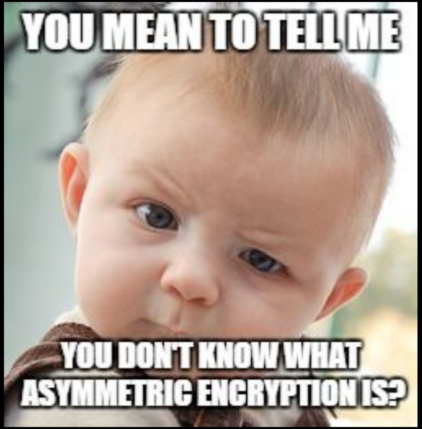
XOR IS A LOGICAL OPERATION
NOT SOME CRYPTOGRAPHIC MAGIC SAUCE TURNING DUST INTO SECURITY
imgflip.com



PLAINTEXT → CIPHERTEXT → PLAINTEXT

S.H.E.L.L.
SECURITY IS AN ILLUSION

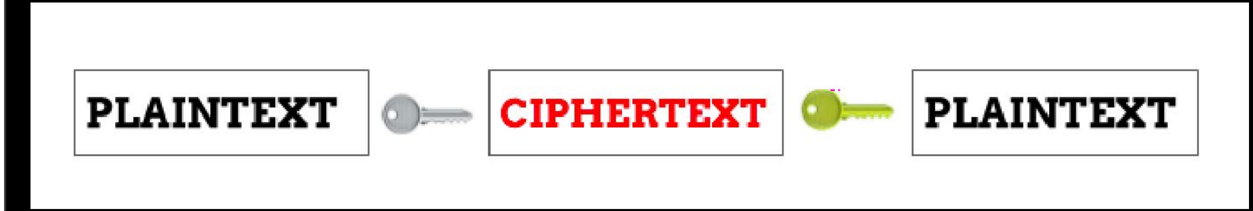
Asymmetric



Asymmetric Encryption

- Two keys – Public(to encrypt) and Private(to decrypt) key
- The private key needs to be hidden and public key can be openly disclosed
- Slower than symmetric, used to protect small but important data.
- Ex: RSA, Diffie -Hellman key exchange, elliptical curve cryptography etc.

This is harder to decrypt than symmetric



PLAINTEXT → CIPHERTEXT → PLAINTEXT

S.H.E.L.L.

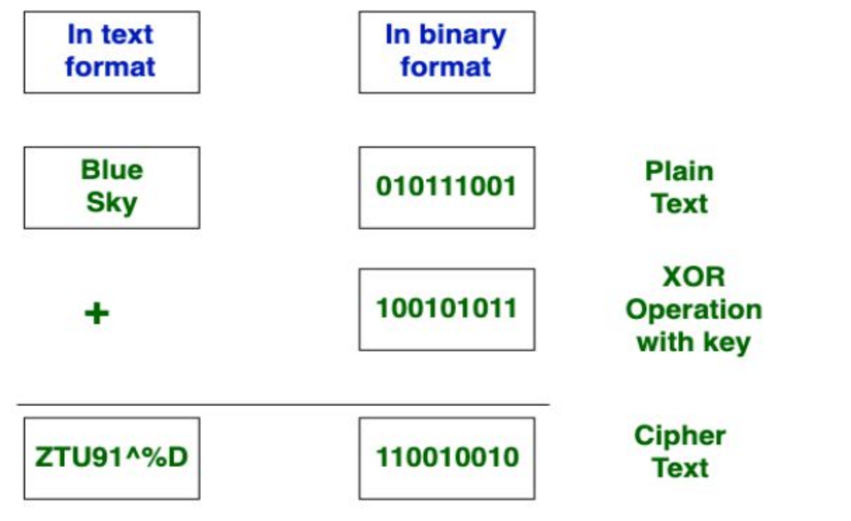
SECURITY IS AN ILLUSION

Encryption Techniques

Stream Ciphers

Stream Cipher

- Stream Cipher Converts the plain text into cipher text by taking 1 char of plaintext.
- Works on 1 byte / 8 bits at a time.

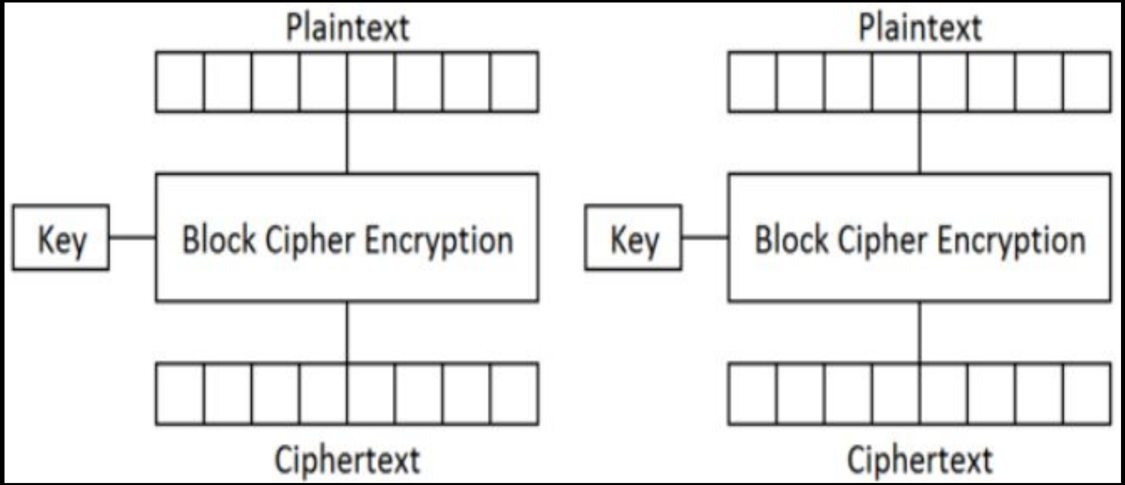


In text format	In binary format	
Blue Sky	010111001	Plain Text
+	100101011	XOR Operation with key
ZTU91^%D	110010010	Cipher Text

Block Ciphers

Block Cipher

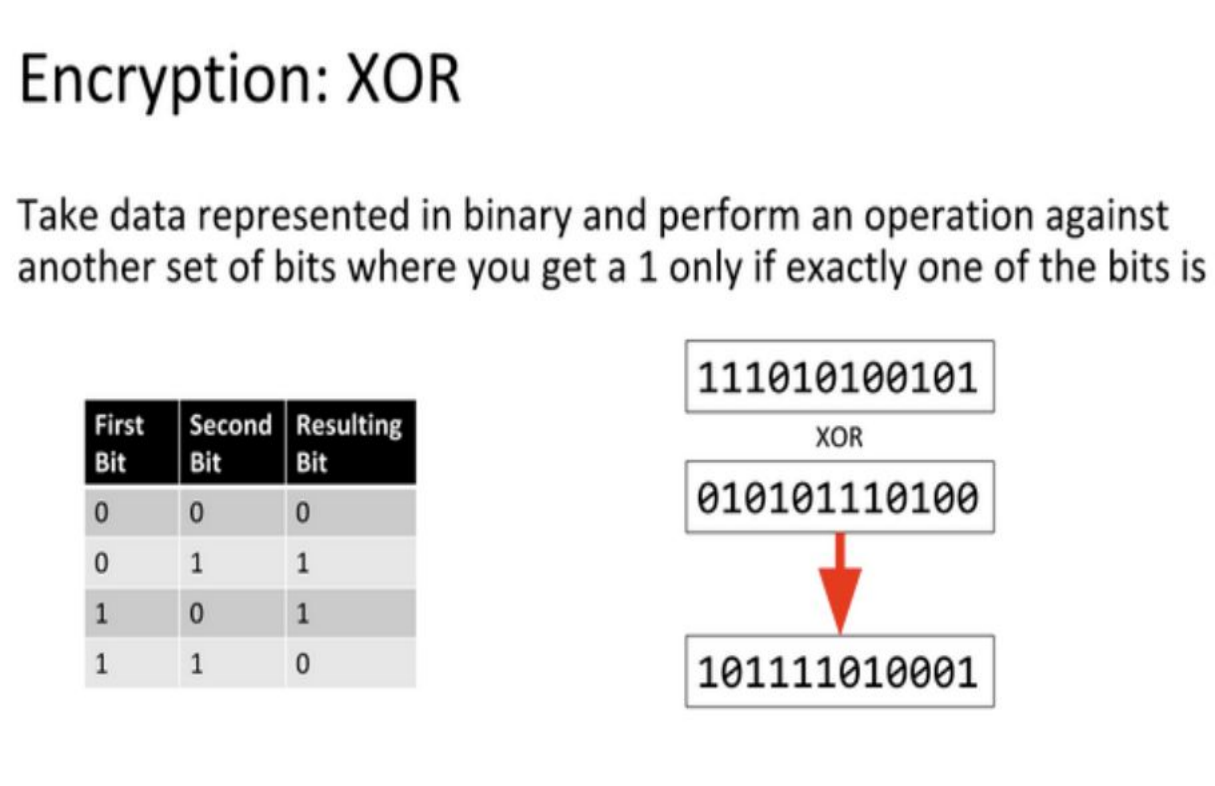
- Block Cipher Converts the plain text into cipher text by taking plain text as blocks at a time.
- Blocks of size 64, 128 and 256 bits
- May have to use padding



S.H.E.L.L.
SECURITY IS AN ILLUSION

XOR

XOR
logic gate
0 0
XOR
logic gate
0 1
XOR
logic gate
1 0
XOR
logic gate
1 1



Encryption: XOR

Take data represented in binary and perform an operation against another set of bits where you get a 1 only if exactly one of the bits is

First Bit	Second Bit	Resulting Bit
0	0	0
0	1	1
1	0	1
1	1	0

111010100101

XOR

010101110100

101111010001

- It’s a symmetric encryption.
- https://ctf101.org/cryptography/what-is-xor/

XOR

There is a technique called bruteforce.

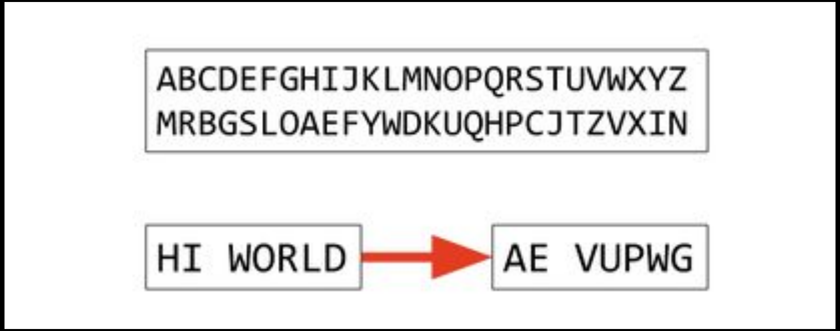
Message: q{vpln'bH_varHuebcrqxetrHOXEj No key! Just brute .. brute .. brute ... :D

Challenge-2

I've hidden some data using XOR with a single byte, but that byte is a secret. Don't forget to decode from hex first.

```
73626960647f6b206821204f21254f7d694f76
24662065622127234f726927756d
```

Substitution Cipher

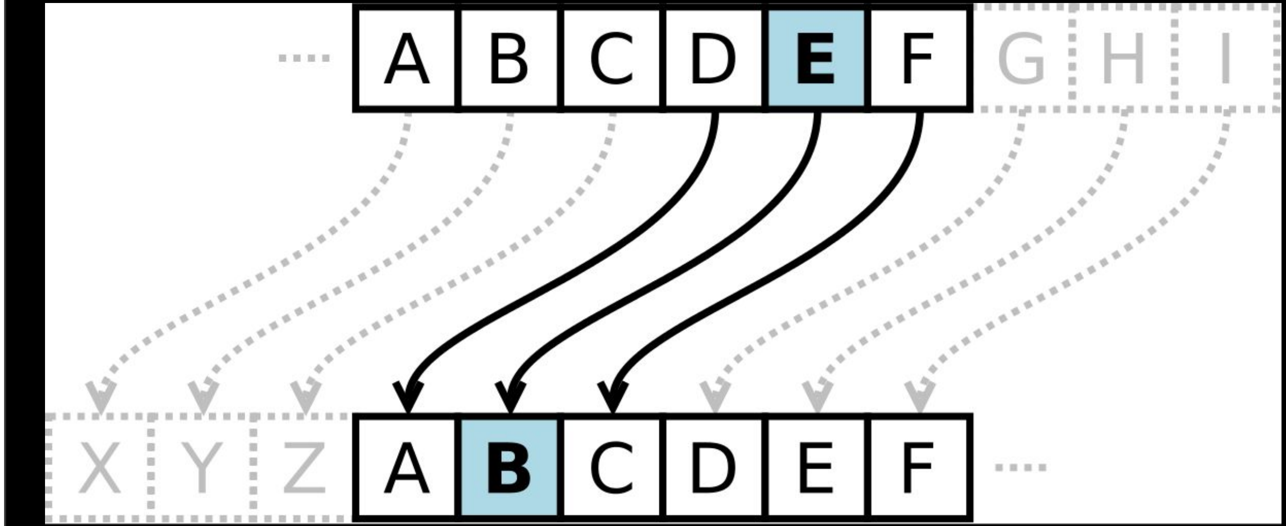


ABCDEFGHIJKLMNOPQRSTUVWXYZ
MRBGSLOAEFYWDKUQHPCJTZVXIN

HI WORLD → AE VUPWG

Shift Cipher

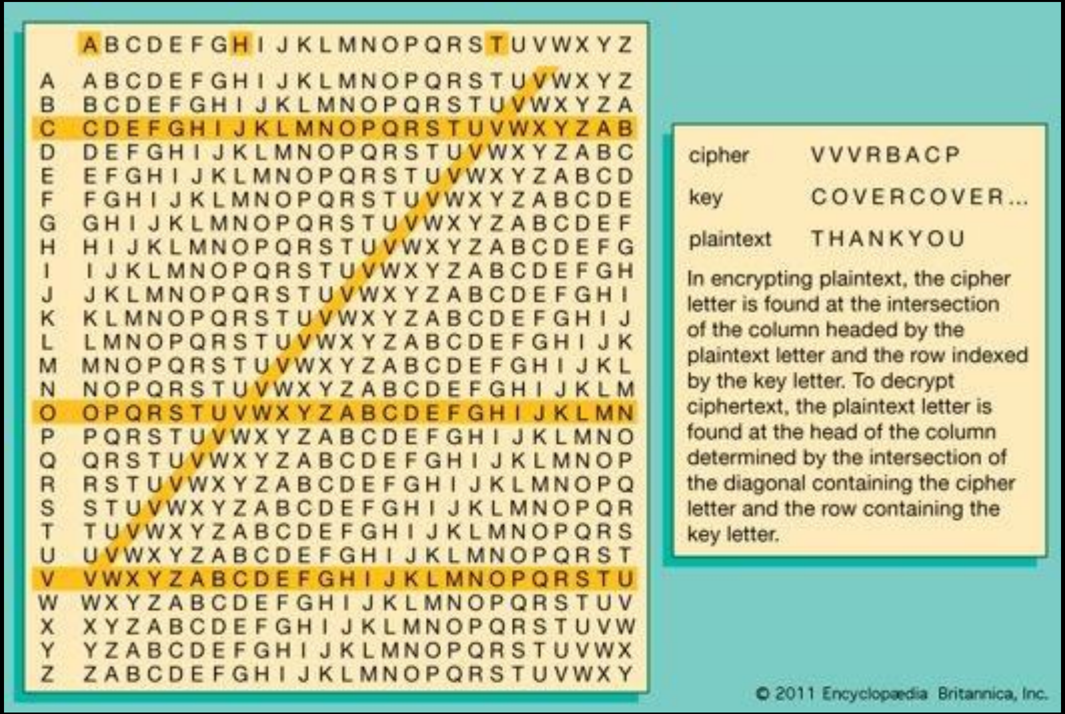
WHEN THEY ASK YOU TO DO CRYPTOGRAPHY
BUT IT'S A CEASAR CIPHER SHIFT OF 2



S.H.E.L.L.

SECURITY IS AN ILLUSION

Vigenere Cipher



	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	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
B	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
C	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
D	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
E	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
F	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
G	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
H	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
I	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
J	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
K	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
L	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
M	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
N	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
O	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
P	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
Q	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
R	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
S	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
T	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
U	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
V	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
W	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
X	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
Y	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
Z	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

cipher	VVVRBACP
key	COVERCOVER...
plaintext	THANKYOU

In encrypting plaintext, the cipher letter is found at the intersection of the column headed by the plaintext letter and the row indexed by the key letter. To decrypt ciphertext, the plaintext letter is found at the head of the column determined by the intersection of the diagonal containing the cipher letter and the row containing the key letter.

Vigenere Cipher

The vigenere cipher is a method of encrypting alphabetic text by using a series of interwoven Caesar ciphers based on the letters of a keyword.<br />

I’m not sure what this means, but it was left lying around: blorpy

gwox{RgqssihYspOntqpxs}

Challenge-3

There are so many different ways of encoding and decoding information nowadays... One of them will work!

Q1RGe0ZsYWdneVdhZ2d5UmFnZ3l9

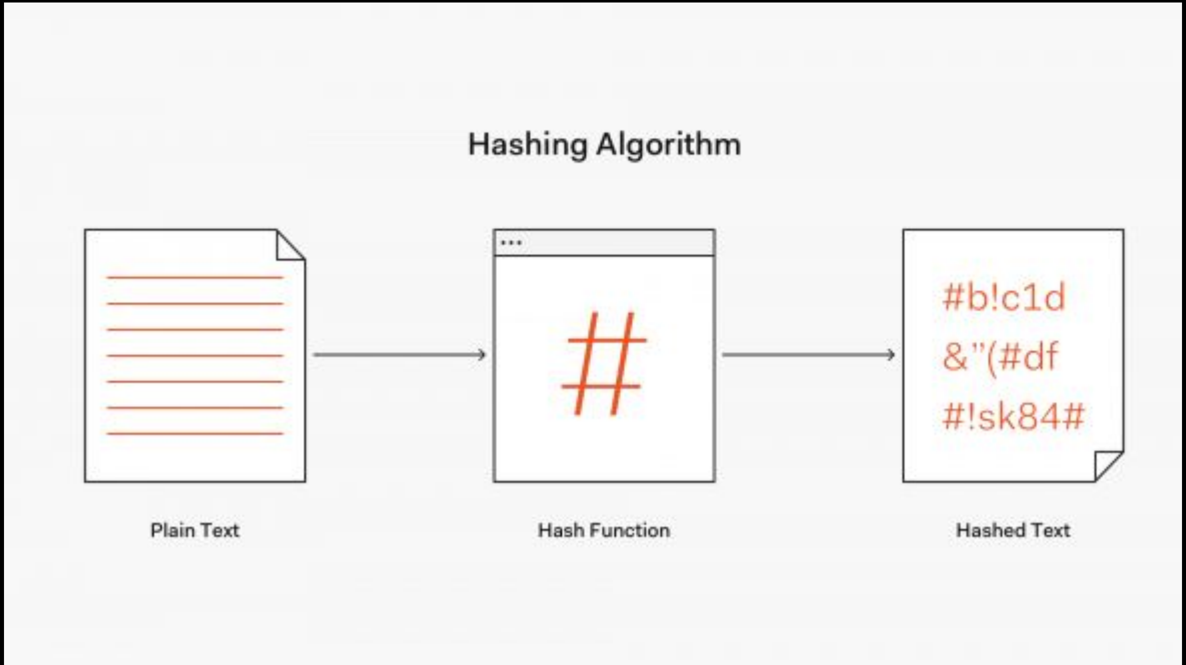
Challenge-4

I got a new hard drive just to hold my flag, but I'm afraid that it rotted. What do I do? The only thing I could get off of it was this:

010000110101010001000110011110110100000100110100
10111010001011111010001100110110001101001011100
00011100000011010010110111001111101

S.H.E.L.L.
SECURITY IS AN ILLUSION

Hashes

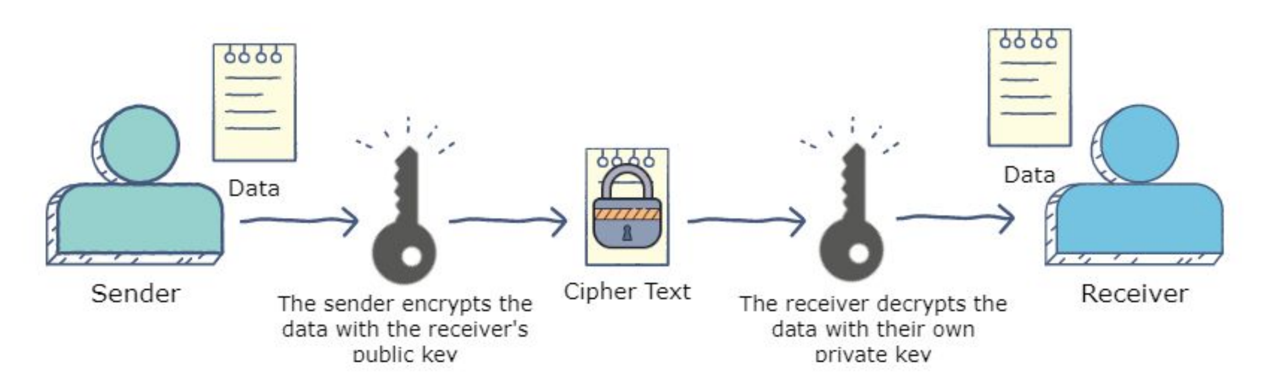


S.H.E.L.L.
SECURITY IS AN ILLUSION

RSA

RSA(Rivest-Shamir-Adleman) is an algorithm used by modern computers to encrypt and decrypt messages.It is an asymmetric cryptographic algorithm.

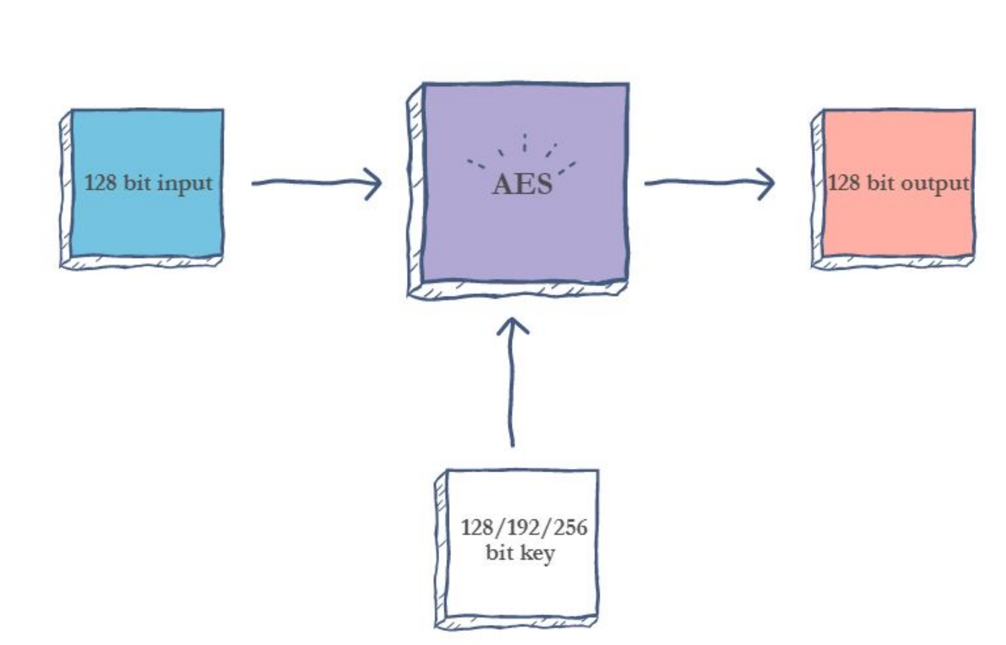
https://www.educative.io/edpresso/what-is-the-rsa-algorithm


Sender
Data
The sender encrypts the data with the receiver's public key
Cipher Text
The receiver decrypts the data with their own private key
Data
Receiver

AES

It is a worldwide standard used in a lot of places. Like wireless communication, file encryption etc.

https://www.educative.io/edpresso/what-is-the-aes-algorithm



Thank You