Cryptography I

ISSS Beginner Series — Pooja Chivukula

Agenda:

- Qualities of Good Encryption Algorithms
- Symmetric Encryption
  - Stream Ciphers (One Time Pad)
  - Block Ciphers (ECB, CBC)
  - Practice Problems
- Asymmetric Encryption

Some Vocabulary

- **Plain Text:** original form of a message
- **Cipher Text:** encrypted form of a message
- **Key:** specifies a set of rules to transform the plaintext into the cipher text
- **Encryption:** process of concealing the message of a text, through a key
- **Decryption:** process of recovering the message from a cipher text, using a key

Objective-

Eavesdroppers should not gain any additional information even if they intercept messages being exchanged.

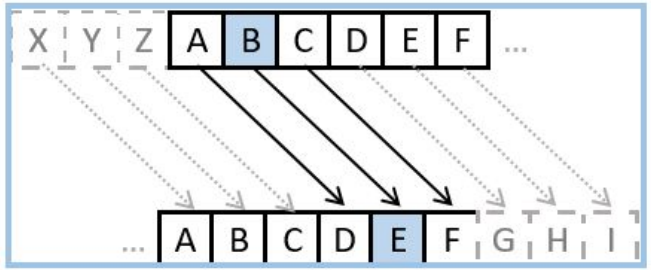
Qualities of Good Encryption Algorithms

- Almost every strong encryption algorithm is theoretically breakable
- For a good encryption algorithm there will be no better alternative to decrypting than brute forcing the different key options

But when are there alternatives to brute-forcing encryption algorithms?

Weak Encryption Algorithm: Caesar Cipher

- Caesar Cipher is a very simple encryption technique that chooses an arbitrary number that it uses to shift the alphabet over and then substitutes the values



SHIFT +3

This Caesar cipher has a shift of 3 characters.

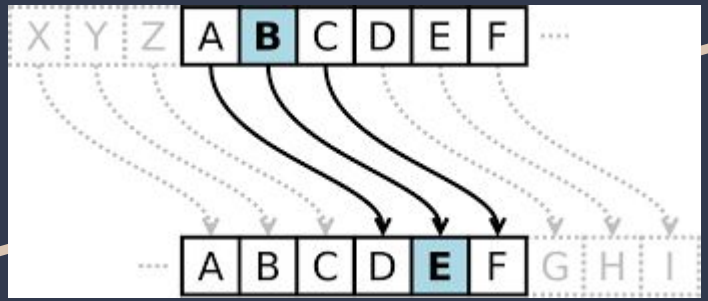
The letter ‘A’ becomes a ‘D’. The letter ‘B’ becomes ‘E’.

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
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

Plaintext

Ciphertext

Why is Caesar Cipher considered a Weak Encryption?



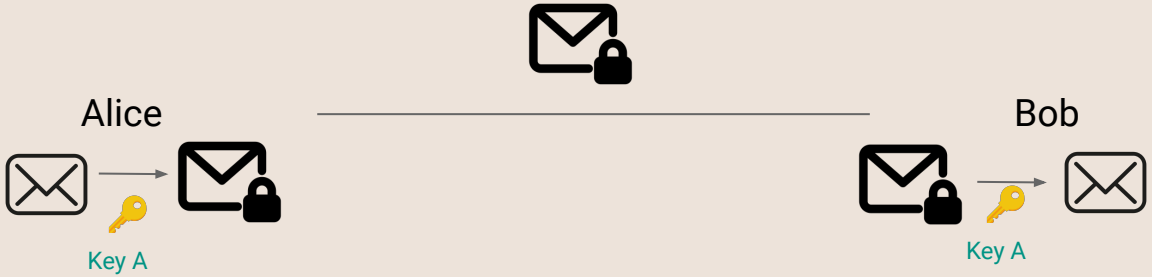
- EX. If you know that E is the most common letter in the English alphabet
  - Knowing this you could find what the most common letter in the encryption test is, and assume it is actually E, and figure out what the shift is.
    - Also known as **frequency analysis**
    - The more ciphertext you have the easier it is to crack the encryption
  - Thus, we have reduced the key space by making educated guesses

Agenda:

- Qualities of Good Encryption Algorithms
- **Symmetric Encryption**
  - Stream Ciphers (One Time Pad)
  - Block Ciphers (ECB, CBC)
  - Practice Problems
- Asymmetric Encryption

Symmetric Ciphers

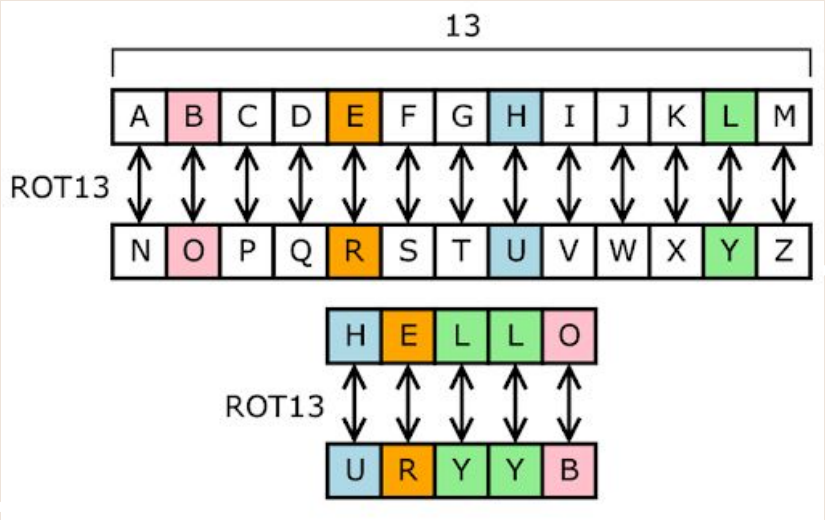
- Same key is used to encrypt and decrypt it
- Two Types: Stream Ciphers & Block Ciphers



Pros	Cons
Simple Calculations, very fast	Key Distribution Problem

Stream Ciphers

- Convert symbols in the text directly (Ex. simple substitution)
- Also known as Substitution Ciphers
- **Confusion:** when the message is disguised by exchanging symbols



Pros	Cons
High Speed of Encryption (typically linear)	Low Diffusion
Simple, less error prone	Susceptible to insertions by attackers

One Time Pad

- A Type of Stream Cipher and is a theoretically perfect cipher
- **Perfect Cipher:** One for which there is no reduction of the search space gained from knowing the following
  - ➔ Encryption Algorithm
  - ➔ Cipher Text
- XOR a random key (that is the same length as the plaintext) with the plaintext

EX.

Key: **0110100010101**
Plaintext: **1110101011010**
Ciphertext: **1000001001111**

So why don't we always use the one time pad?

Why is this so strong?

When an attacker tries to decrypt cipher text, there are 2^n possible plaintexts that could be the pre-image of the cipher text under a plausible key

Fatal Flaw in One Time Pad

- Problem with one time pad is that it only works for one message exchange
- If you create a new key for every iteration
  - you would need a secure channel to exchange that key
  - The key is the same length as the message
  - at that point you could just exchange the message itself ->*key exchange problem*

Why can we only use it once?

1st Round of Encryption: $m_1 \oplus k$

2nd Round of Encryption: $m_2 \oplus k$

$$(m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$$

Hence, there is memory leakage.

There is a approximate one time pad that solves this issue. *(Vernam Cipher)*

Problem #1:

Someone stole my super secret flag, and added something to each character to make it encoded with "EMOJII"!I've heard of ASCII, but what's EMOJII?

Oh by the way, he left a note saying his favorite number is 0x1f400, not sure what that means...

https://tinyurl.com/cryptoOne

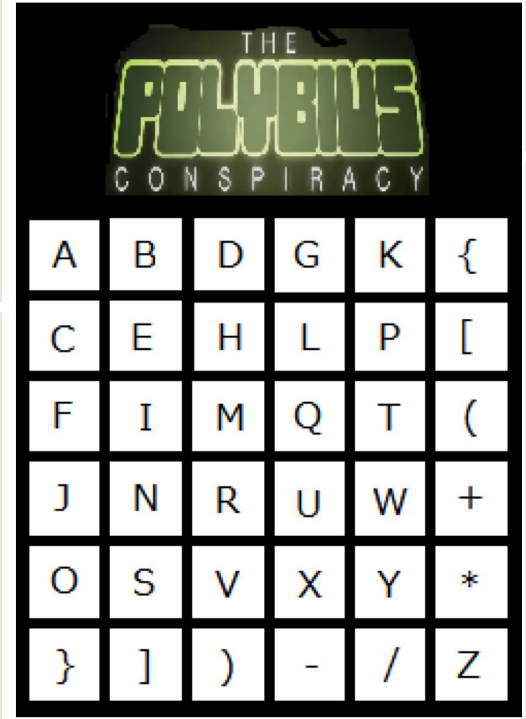
Credit for writing this problem goes to Steven!

Problem #2:

Someone told me about this game that drives people insane, gave me this number, and told me it starts with ut.

44 35 31 24 11 14 16 13 51 64 42 51 35 64 25 11 52 52 64 14 51 64 13 51 64 42 51 35 64 21 51 24 24 22 21 35 64 52 11 42 32 35 55 61

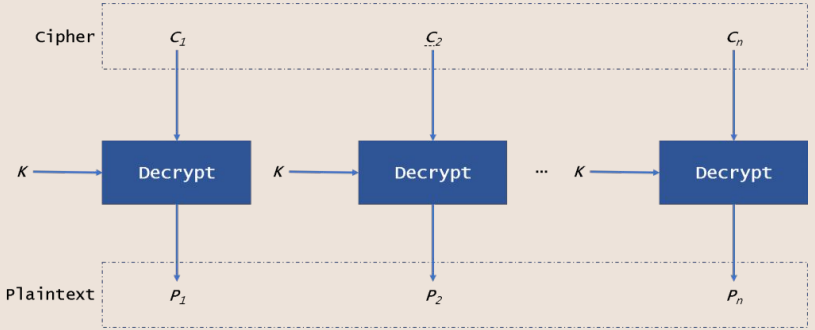
"flag is all lower case" maybe



https://tinyurl.com/cryptoOne

Credit for writing this problem goes to Rob!

Block Ciphers



- Encrypt a group of text as one block
- Modern Block sizes are about 128 bits
- EX.RSA,ECB, CBC
- **Diffusion:** Change the placement of the symbols
  - Often achieved with matrix transposition

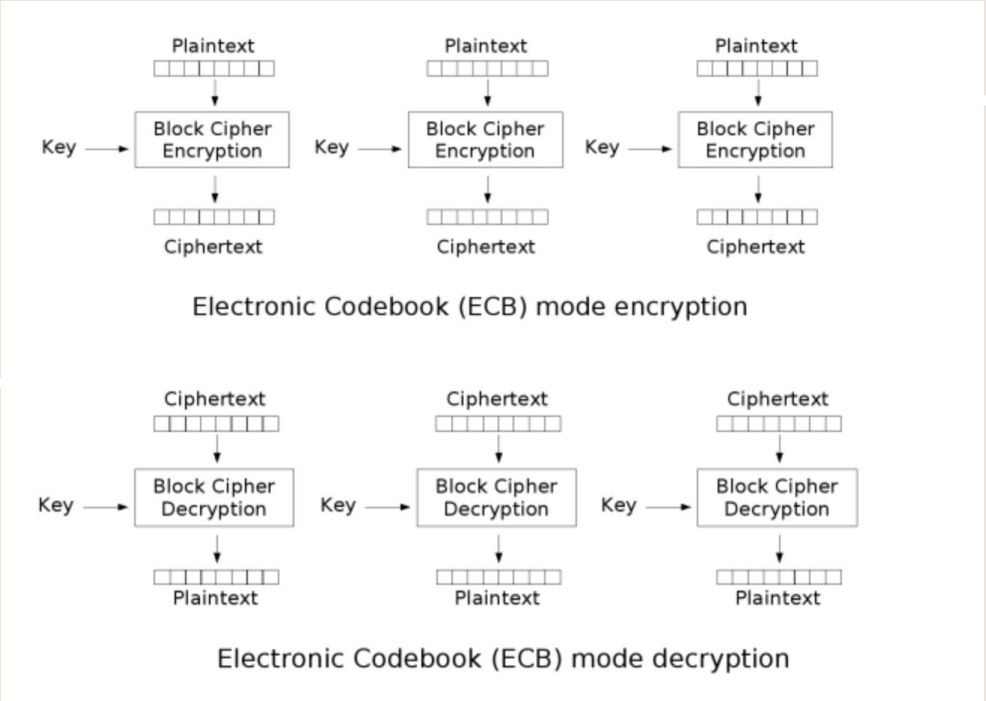
Message: JAMESBONDNEEDSBACKUP
Code: JEONDAUASNESCPMBDEBK

J	E	O	N	D	A	U
A	S	N	E	S	C	P
M	B	D	E	B	K	

Pros	Cons
High Diffusion	Slow Encryption/Decryption
Harder to Tamper with	Error Prone

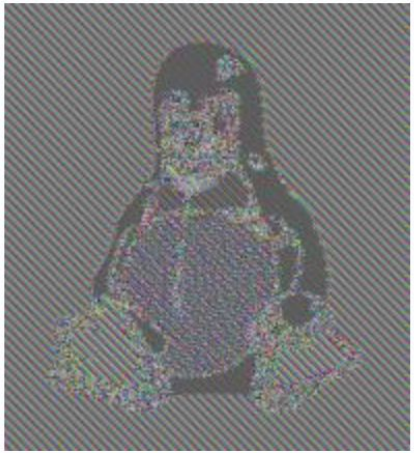
Electronic Codebook (ECB)

- Most simple block cipher
- Chunks up plaintext and encodes each chunk *INDEPENDENTLY*



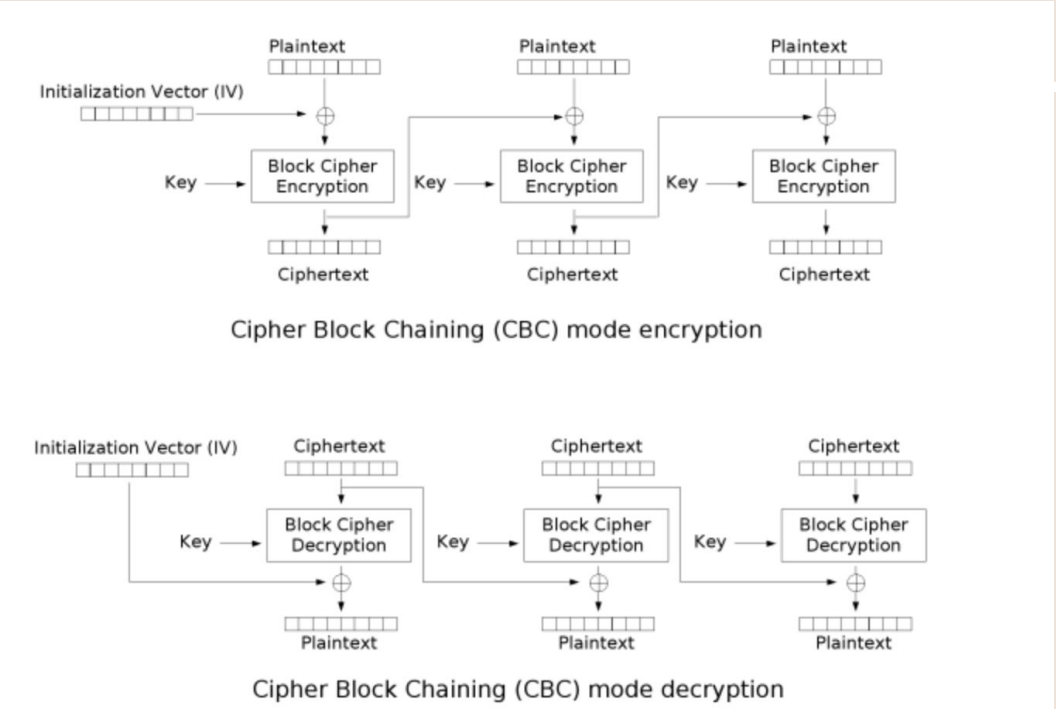
Electronic Codebook (EBC) - Flaw

- Because it encodes each chunk independently, patterns in the plaintext can still be seen

Original Image	ECB Image	Other Block Cipher Modes
		

Cipher Block Chaining (CBC)

- Can solve this issue by introducing son randomness
  - CBC introduces an initialization vector



Ok so... we now know that encryption requires a key... and the key has to be kept private...

So how do we get the key from person A to person B without it getting leaked??

Hence....

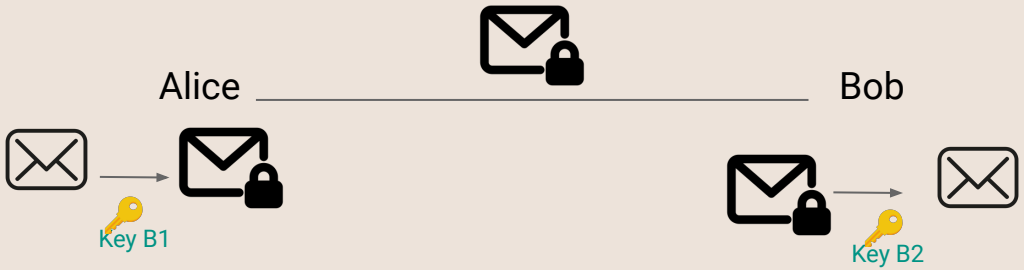
The Key Distribution Problem.

Agenda:

- Qualities of Good Encryption Algorithms
- Symmetric Encryption
  - Stream Ciphers (One Time Pad)
  - Block Ciphers (ECB, CBC)
  - Practice Problems
- **Asymmetric Encryption**

Asymmetric Ciphers

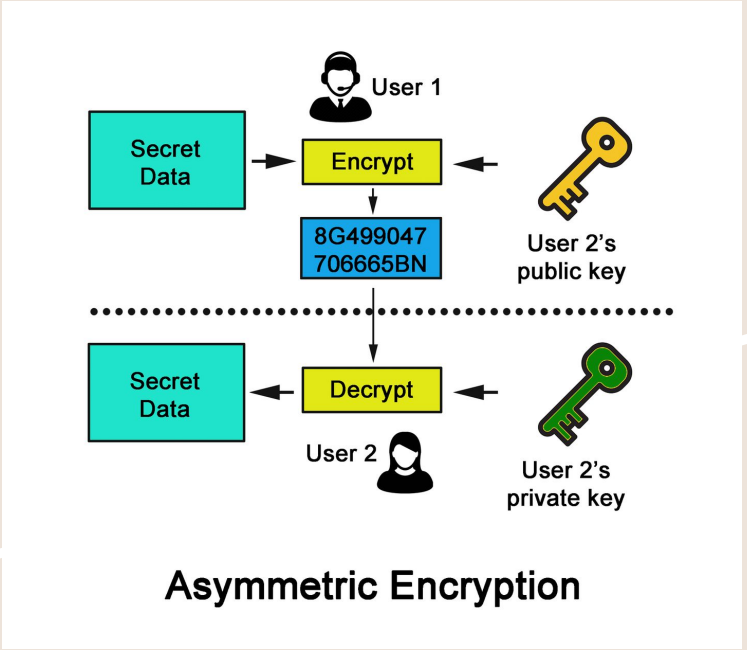
- Different key is used to encrypt and decrypt it



Say Bob has 2 keys B1 which is public (everyone has access to), and B2 which is private (only he has access to)

Asymmetric Ciphers

- Each subject S has a publicly disclosed key (***public key***) that anyone can use to encrypt a plaintext and a ***private key*** that only they can use to decrypt the ciphertext



Asymmetric Encryption

Pros	Cons
Solves the key distribution problem	**Expensive** to generate public keys, (keys usually involve large prime numbers because is no polynomial time algorithm to factor prime numbers)

Asymmetric Ciphers

- Different key is used to encrypt and decrypt it

Alice  Bob

Bob's Keys:
B1 — Public
B2 — Private

Alice's Keys:
A1 — Public
A2 — Private

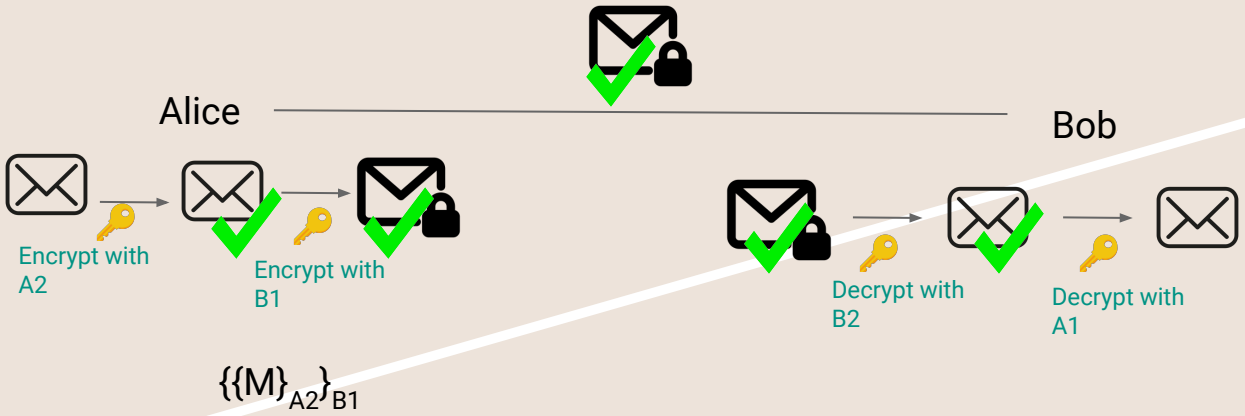
- Using this how can Bob verify that Alice sent the message? I.E how can Alice sign her message?

Asymmetric Ciphers

Bob's Keys:
B1 — Public (encryption)
B2 — Private (decryption)

Alice's Keys:
A1 — Public (decryption)
A2 — Private (encryption)

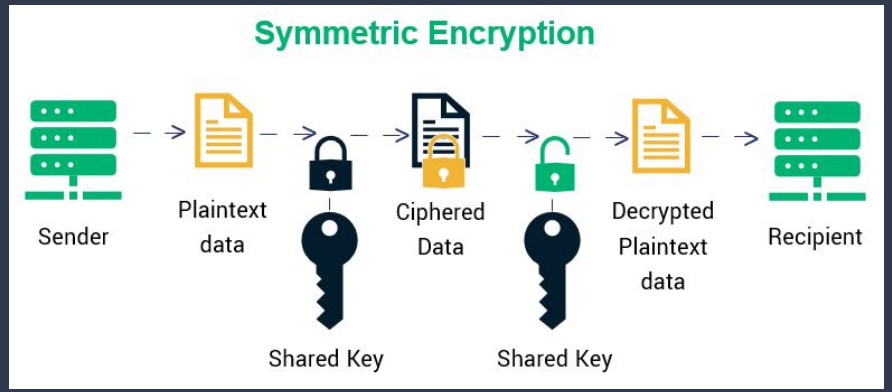
- Different key is used to encrypt and decrypt it



- Here Alice's private key is used to SIGN (and authenticate) her message

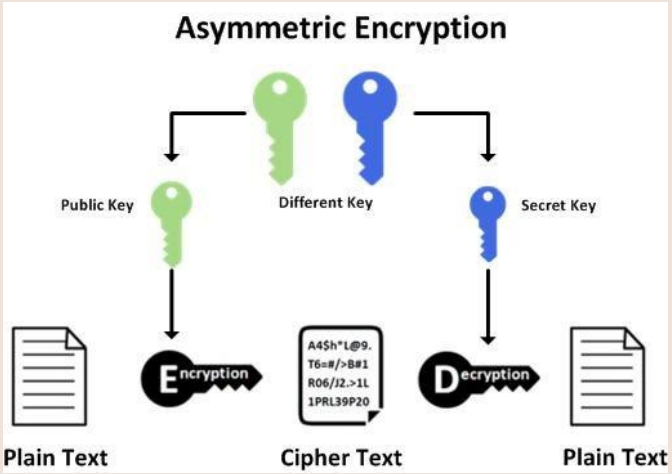
Symmetric

- Same key is used to encrypt and decrypt messages
- Generally involves a randomly generated k-bit string of characters for the key
- EX. AES, DES, TLS



Asymmetric

- Same key is not used to encrypt and decrypt a message
- Involves a private and public key
- EX. RSA, Diffie Hellman



Questions?