

# CRYPTANALYSIS

CRYPTANALYSIS in cryptography

By

Avijit Banarjee



# INTRODUCTION

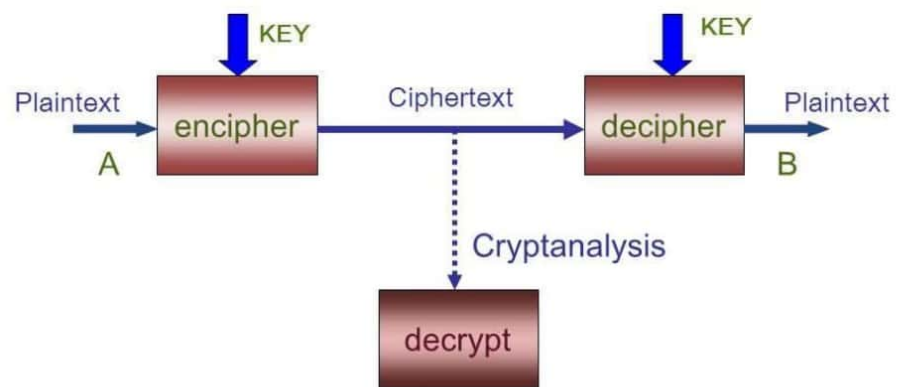
cryptanalysts seek to decrypt ciphertexts without knowledge of the plaintext source, encryption key or the algorithm used to encrypt it



# GOAL

cryptanalysts' research results are used by cryptographers to improve and strengthen or replace flawed algorithms

## The general cryptographic procedure



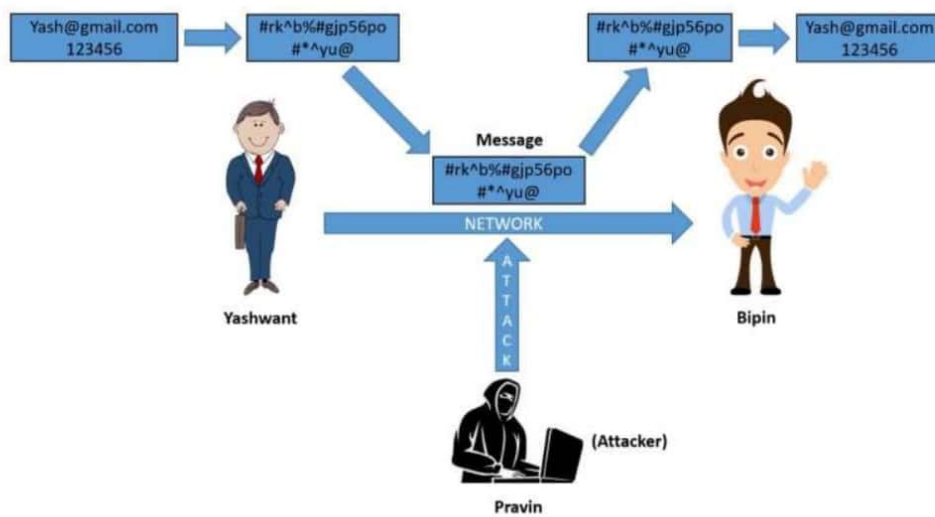
# Cryptanalysis

- objective to recover key not just message
- general approaches:
  - cryptanalytic attack
  - brute-force attack

## Why cryptanalysis

cryptanalysis is practiced by a broad range of organizations  
Including

- governments aiming to decipher other nations' confidential communications
- companies developing security products that employ cryptanalysts to test their security features etc.



# **CRYPTANALYSIS ATTACKS**



# Cryptanalytic Attacks

## ➤ ciphertext only

- only know algorithm & ciphertext, is statistical, know or can identify plaintext

## ➤ known plaintext

- know/suspect plaintext & ciphertext

## ➤ chosen plaintext

- select plaintext and obtain ciphertext

## ➤ chosen ciphertext

- select ciphertext and obtain plaintext

## ➤ chosen text

- select plaintext or ciphertext to en/decrypt

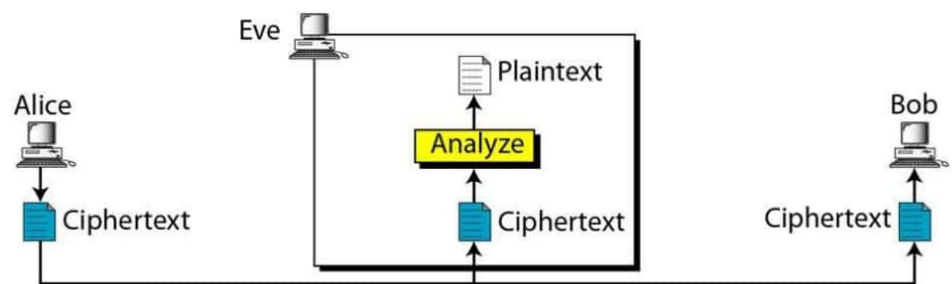
## ***ciphertext-only attack***

The attacker only has access to one or more encrypted messages but knows nothing about the plaintext data

- ▣ the encryption algorithm being used
- ▣ any data about the cryptographic key being used

This is the type of challenge that intelligence agencies often face when they have intercepted encrypted communications from an opponent

## Ciphertext-Only Attack



## ***known plaintext attack***

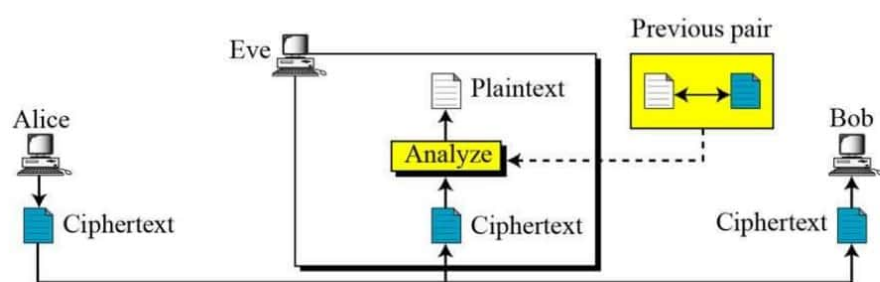



The analyst may have access to some or all of the plaintext of the ciphertext.



The analyst's goal in this case is to discover the key used to encrypt the message and decrypt the message. Once the key is discovered, an attacker can decrypt all messages that had been encrypted using that key.

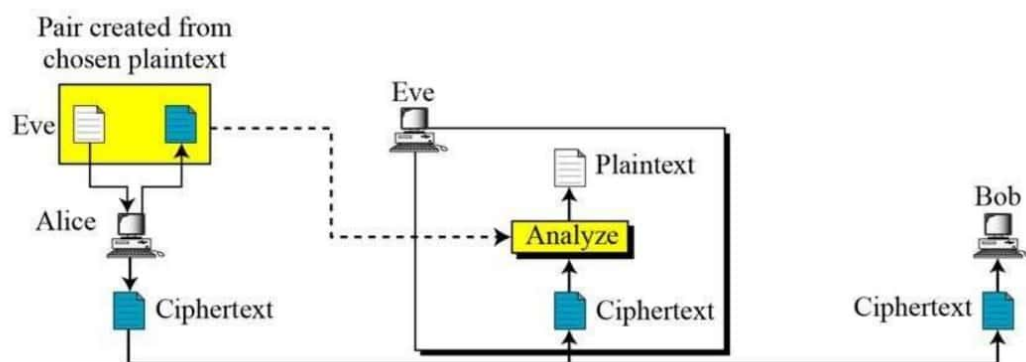
## Known-Plaintext Attack





## ***chosen plaintext attack***

The analyst either knows the encryption algorithm or has access to the device used to do the encryption. The analyst can encrypt the chosen plaintext with the targeted algorithm to derive information about the key



# **Dictionary attack**

- a technique typically used against password files and exploits the human tendency to use passwords based on natural words or easily guessed sequences of letters or numbers



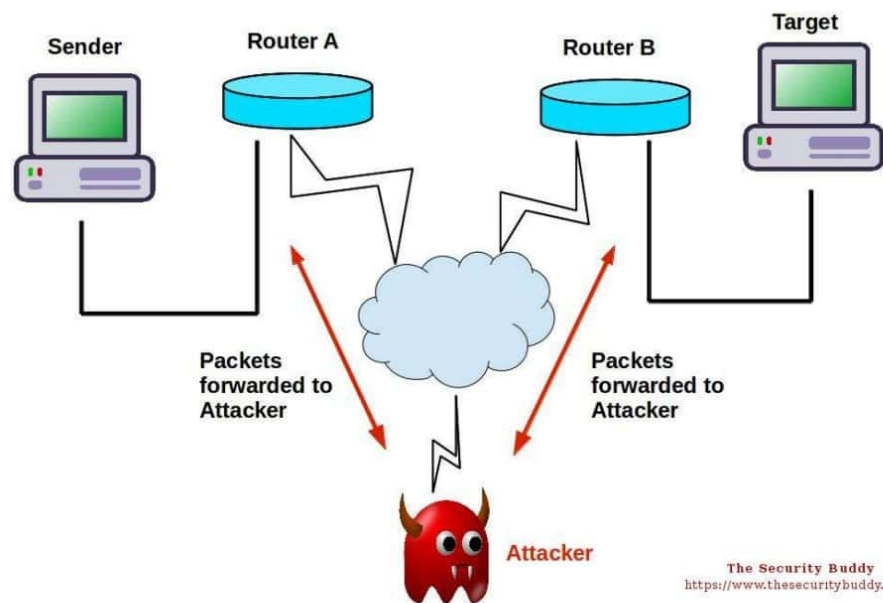
```
Command Prompt
Trying password: 'florida'
Trying password: 'mistress'
Trying password: 'bitch'
Trying password: 'house'
Trying password: 'beer'
Trying password: 'eric'
Trying password: 'phantom'
Trying password: 'hello'
Trying password: 'miller'
Trying password: 'rocket'
Trying password: 'legend'
Trying password: 'billy'
Trying password: 'scooter'
Trying password: 'flower'
Trying password: 'theman'
Trying password: 'movie'
Trying password: '6666'
Trying password: 'please'
Trying password: 'jack'
Trying password: 'oliver'

Password has been found. Your password is 'Password'
C:\Users\Owner\Desktop\KeePass>
```

## *Man-in-the-middle attacks*

- occur when cryptanalysts find ways to insert themselves into the communication channel between two parties who wish to exchange their keys for secure communication via asymmetric or public key infrastructure. The attacker then performs a key exchange with each party, with the original parties believing they are exchanging keys with each other. The two parties then end up using keys that are known to the attacker.

## Man-In-The-Middle Attack



# Brute Force Attack

- A **brute force attack** is any type of attack that involves trying every possible combination of characters or data in order to find the key in order to decrypt an encrypted message.
- A brute force attack is usually used as a last-resort tactic in a cryptanalysis scenario, as it very much involves extreme amounts of trial and error and relies on a lot of luck in order to find the key. A brute force attack is different from a dictionary attack, as it does not rely on a dictionary and simply tries every possible key that could be used.

# Brute Force Search

- always possible to simply try every key
- most basic attack, proportional to key size
- assume either know / recognise plaintext

Key Size (bits)	Number of Alternative Keys	Time required at 1 decryption/ $\mu$ s	Time required at $10^6$ decryptions/ $\mu$ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu$ s = 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu$ s = 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu$ s = $5.4 \times 10^{24}$ years	$5.4 \times 10^{18}$ years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu$ s = $5.9 \times 10^{36}$ years	$5.9 \times 10^{30}$ years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu$ s = $6.4 \times 10^{12}$ years	$6.4 \times 10^6$ years

File Edit View Window Help

```
* 192.168.0.197:3306 MySQL - [56/72] - Trying username:'ashishi' with password:'1212'
* 192.168.0.197:3306 MySQL - [56/72] - failed to login as 'ashishi' with password '1212'
* 192.168.0.197:3306 MySQL - [57/72] - Trying username:'ashishi' with password:'123321'
* 192.168.0.197:3306 MySQL - [57/72] - failed to login as 'ashishi' with password '123321'
* 192.168.0.197:3306 MySQL - [58/72] - Trying username:'ashishi' with password:'hello'
* 192.168.0.197:3306 MySQL - [58/72] - failed to login as 'ashishi' with password 'hello'
* 192.168.0.197:3306 MySQL - [59/72] - Trying username:'gelowo' with password:'12121'
* 192.168.0.197:3306 MySQL - [59/72] - failed to login as 'gelowo' with password '12121'
* 192.168.0.197:3306 MySQL - [60/72] - Trying username:'gelowo' with password:'asdad'
* 192.168.0.197:3306 MySQL - [60/72] - failed to login as 'gelowo' with password 'asdad'
* 192.168.0.197:3306 MySQL - [61/72] - Trying username:'gelowo' with password:'asdasd'
* 192.168.0.197:3306 MySQL - [61/72] - failed to login as 'gelowo' with password 'asdasd'
* 192.168.0.197:3306 MySQL - [62/72] - Trying username:'gelowo' with password:'asdas'
* 192.168.0.197:3306 MySQL - [62/72] - failed to login as 'gelowo' with password 'asdas'
* 192.168.0.197:3306 MySQL - [63/72] - Trying username:'gelowo' with password:'1212'
* 192.168.0.197:3306 MySQL - [63/72] - failed to login as 'gelowo' with password '1212'
* 192.168.0.197:3306 MySQL - [64/72] - Trying username:'gelowo' with password:'123321'
* 192.168.0.197:3306 MySQL - [64/72] - failed to login as 'gelowo' with password '123321'
* 192.168.0.197:3306 MySQL - [65/72] - Trying username:'gelowo' with password:'hello'
* 192.168.0.197:3306 MySQL - [65/72] - failed to login as 'gelowo' with password 'hello'
* 192.168.0.197:3306 MySQL - [66/72] - Trying username:'root' with password:'12121'
* 192.168.0.197:3306 MySQL - [66/72] - failed to login as 'root' with password '12121'
* 192.168.0.197:3306 MySQL - [67/72] - Trying username:'root' with password:'asdad'
* 192.168.0.197:3306 MySQL - [67/72] - failed to login as 'root' with password 'asdad'
* 192.168.0.197:3306 MySQL - [68/72] - Trying username:'root' with password:'asdasd'
* 192.168.0.197:3306 MySQL - [68/72] - failed to login as 'root' with password 'asdasd'
* 192.168.0.197:3306 MySQL - [69/72] - Trying username:'root' with password:'asdas'
* 192.168.0.197:3306 MySQL - [69/72] - failed to login as 'root' with password 'asdas'
* 192.168.0.197:3306 MySQL - [70/72] - Trying username:'root' with password:'1212'
* 192.168.0.197:3306 MySQL - [70/72] - failed to login as 'root' with password '1212'
* 192.168.0.197:3306 MySQL - [71/72] - Trying username:'root' with password:'123321'
* 192.168.0.197:3306 MySQL - [71/72] - failed to login as 'root' with password '123321'
* 192.168.0.197:3306 MySQL - [72/72] - Trying username:'root' with password:'hello'
* 192.168.0.197:3306 - SUCCESSFUL LOGIN 'root' : 'hello'
```