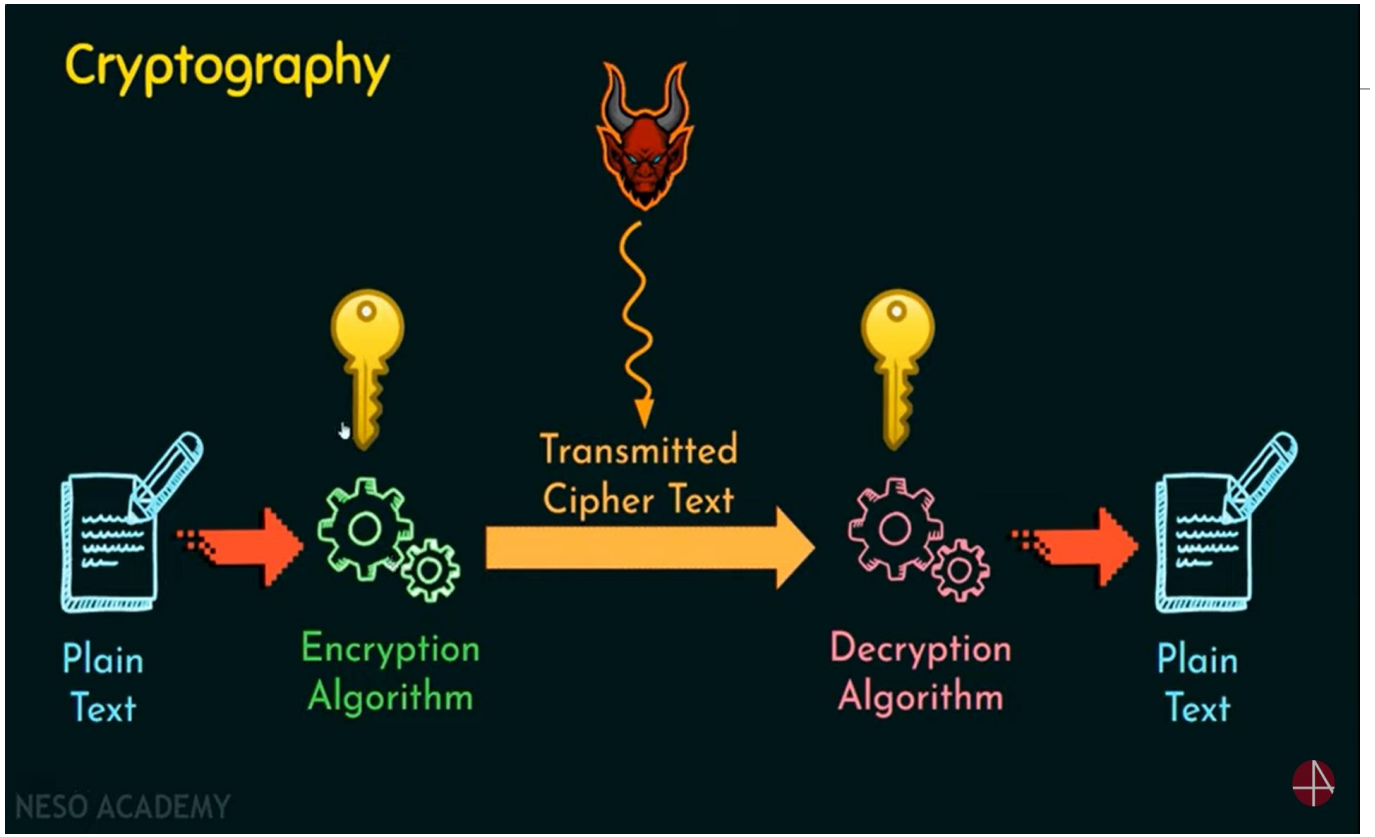
CRYPTOGRAPHY



Lecture two

CRYPTOGRAPHY VS CRYPTOANALYSIS

Assist prof. Dr. Saja J. Mohammed

Course reference:
CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE-SEVENTH EDITION / by William Stallings

Cryptography

- Cryptography is the study and application of mathematical constructs and protocols to provide mechanisms for securing data and communication from eavesdroppers.
- It is the art of keeping information secure by transforming data into a form that unauthorized recipients cannot understand. In cryptography, an original human-readable message, referred to as plaintext, is changed by means of an algorithm, or series of mathematical operations, into something that to an unreadable formula which is called ciphertext.
- Two forms of cryptography exist: symmetric and asymmetric cryptography
- Symmetric key cryptography utilizes shared keys or secrets with fast ciphers to encrypt and decrypt messages.
- Asymmetric key cryptography utilizes computationally complex math problems to enable encryption and decryption while communicating parties have different keys.
- **The trade-off** of the two types is that symmetric encryption is faster than asymmetric key cryptography , but requires some method of securely sharing the key material. Best practice methodology utilized the strengths of asymmetric cryptography to exchange the secret key between communicating parties so that they may then use the faster symmetric cryptography for data exchange.

Cryptanalysis

- **Cryptanalysis** (also referred to as **codebreaking** or **cracking the code**)
- The term “cryptanalysis” is derived from the Greek words kryptós (meaning “hidden”) and analein (meaning “analysis”).
- It is the process of studying cryptographic systems to look for weaknesses or leaks of information. It try to get the plaintext from ciphertext without decryption key.
- **Cryptanalysis** is used **to break** up authentication schemes, **to break** cryptographic protocols, and **to find and correct** weaknesses in encryption algorithms (ethical use).
- The person practicing Cryptanalysis is called a **Cryptanalyst**.

Who Uses Cryptanalysis?

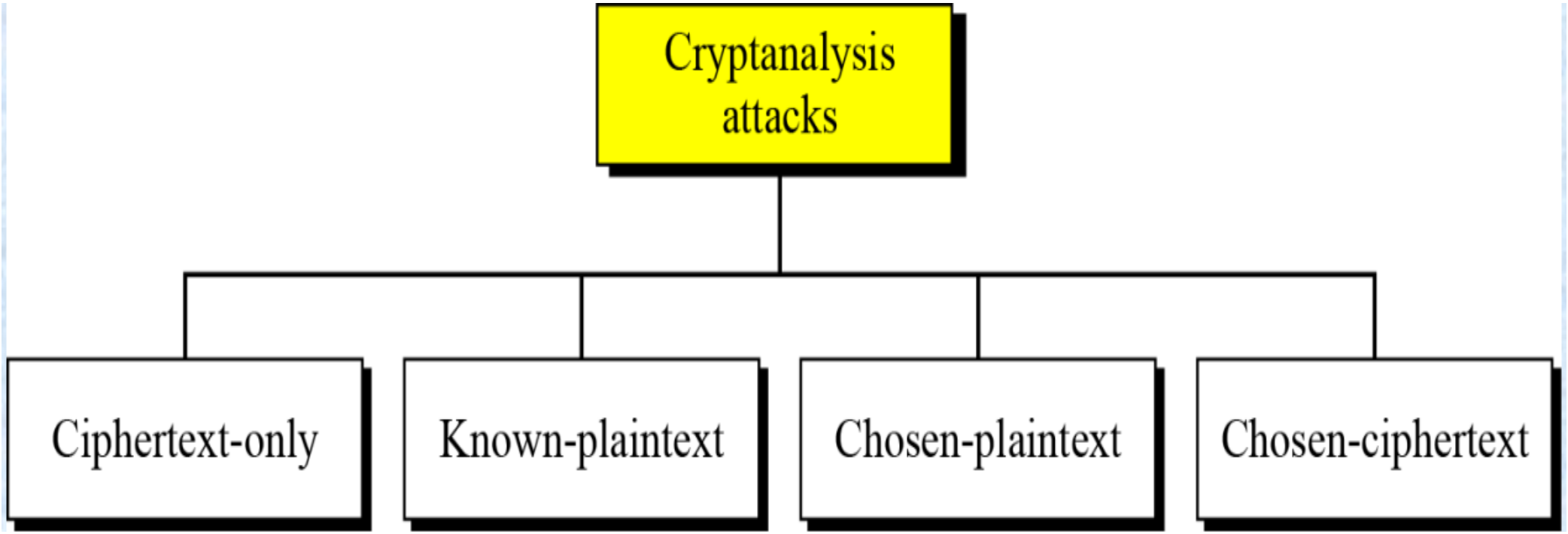
- hackers use cryptanalysis. It is possible, hackers use cryptanalysis to eliminate cryptosystem vulnerabilities rather than a brute force attack.
- Governments use cryptanalysis to decipher the encrypted messages of other nations.
- Companies specializing in cybersecurity products and services use cryptanalysis to test their security features.
- At the world of academia, using cryptoanalysis, researchers and academicians looking for weaknesses in cryptographic algorithms and protocols.
- Both black and white-hat hackers use cryptanalysis.
- **Black-hat** hackers use it to commit cybercrimes, and **white-hat** hackers use it to conduct penetration testing as directed by organizations that hire them to test their security.

Goals of Security

The security mechanisms can:

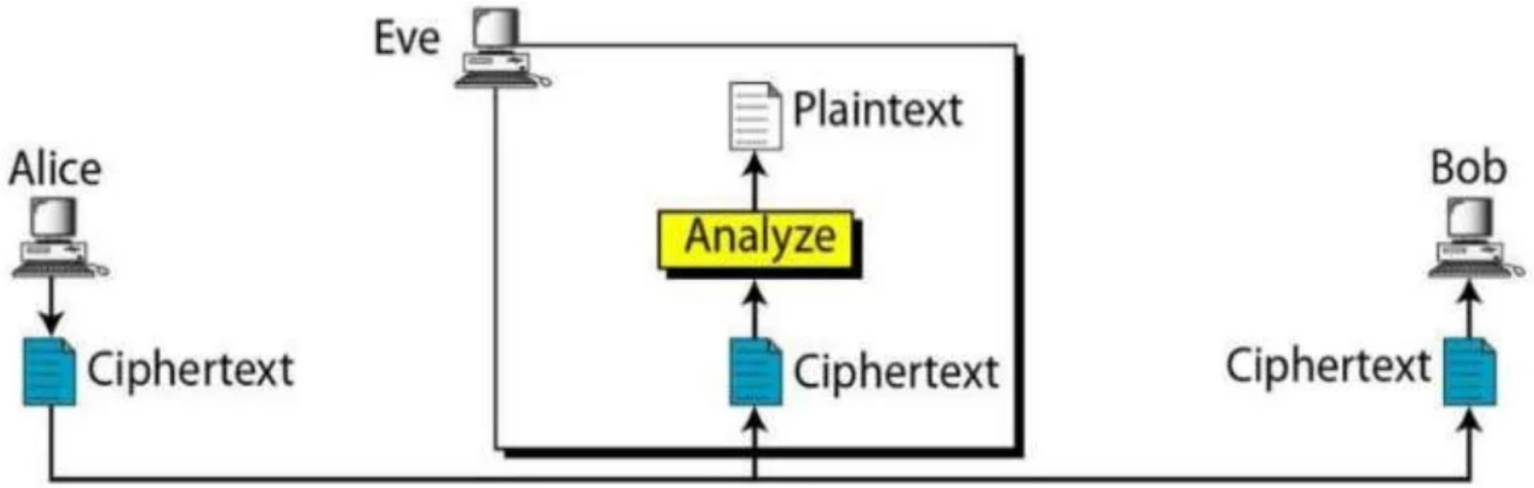
1. Prevent the attack.
2. Detect the attack.
3. Recover from the attack.

Type of cryptanalysis attacks



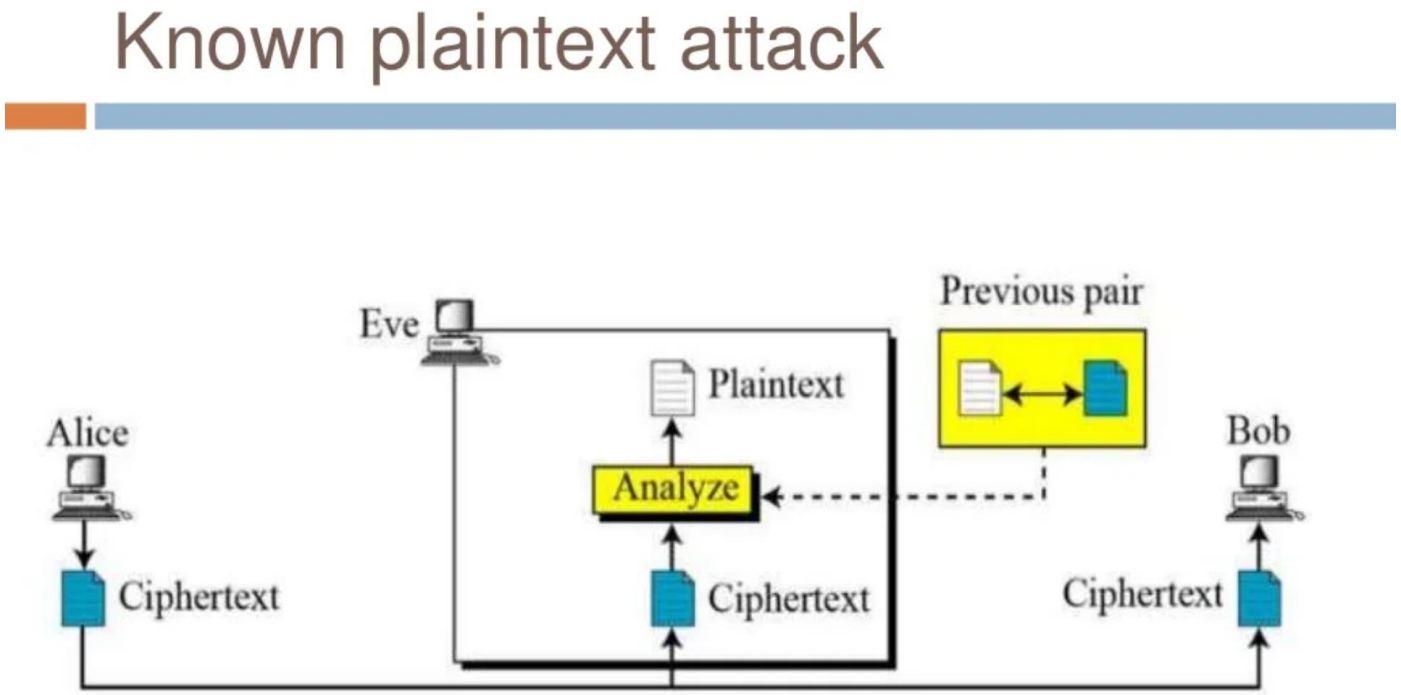
Ciphertext-Only Attack (COA):

In this type of attack, only some ciphertext is known and the attacker tries to find the corresponding encryption key and plaintext.
Its the hardest to implement but is the most probable attack as only ciphertext is required.



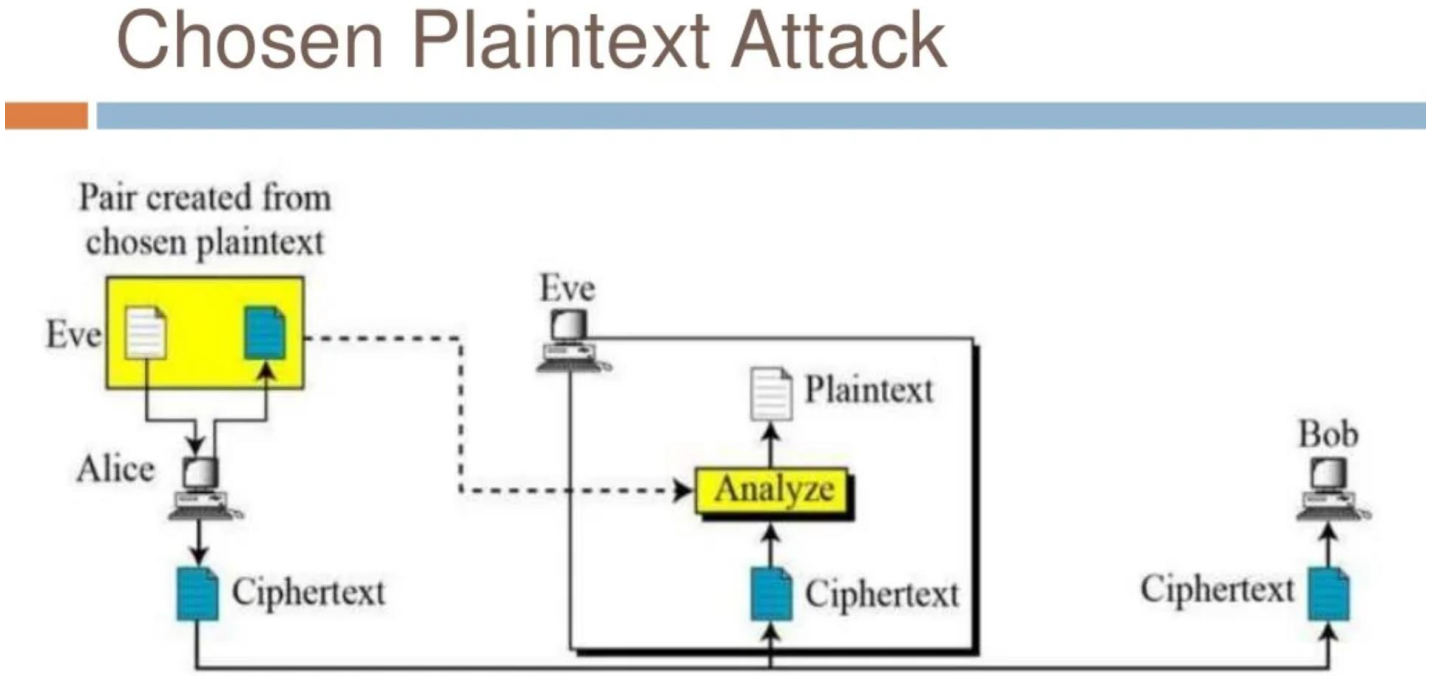
KNOWN-PLAINTEXT ATTACK(KPA)

The attacker is aware of **plaintext-ciphertext pairings** in this case. An attacker just needs to map those pairings to find the encryption key. This attack is quite simple since the attacker already has a wealth of information at his disposal.



Chosen-Plaintext Attack (CPA)

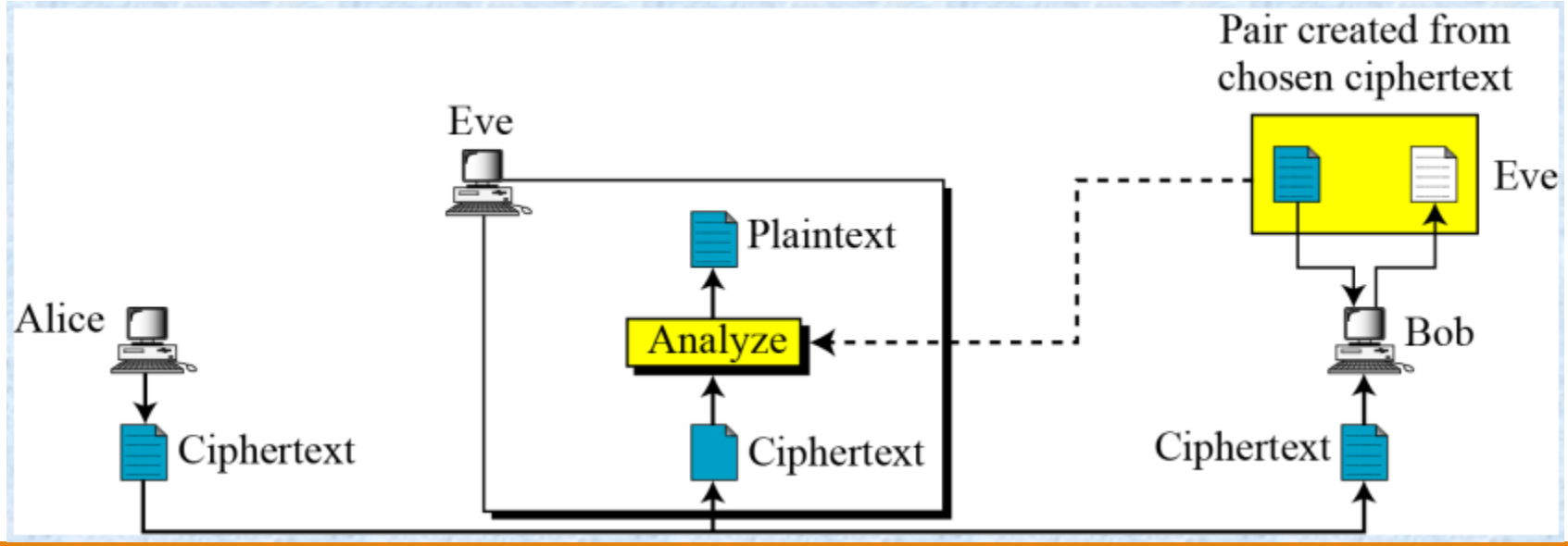
This attack is carried out by selecting random plaintexts and then acquiring the ciphertexts that correspond to them. The encryption key must be discovered by the attacker. Though it is comparable to KPA and is reasonably easy to deploy, it has a low success rate.



chosen-ciphertext attack (CCA)

A **chosen-ciphertext attack** (**CCA**) is an attack model for cryptanalysis where the cryptanalyst can gather information by obtaining the decryptions of chosen ciphertexts. From these pieces of information the adversary can attempt to recover the hidden secret key used for decryption.

Its very simple to implement like KPA but the success rate is quite low.



Type of Attack	Known to Cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext
Known plaintext	•Encryption algorithm •Ciphertext •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Brute force attack

A brute force attack uses trial-and-error to guess login info, encryption keys, During the brute-force attack, the intruder tries all possible keys, and checks which one of them returns the correct plaintext. A brute-force attack is also called **an exhaustive key search**.

An amount of time that is necessary to break a cipher is proportional to the size of the secret key. The maximum number of attempts is equal to

$$2^{\text{key size}},$$

where **key size** is the number of bits in the key.

Brute force attack

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

The success of an attack is depend on

1. The Amount of time available
2. Computing power available
3. Storage capacity available