BRAC UNIVERSITY

Inspiring Excellence

Cryptanalysis

Prepared by:
Dr. Muhammad Iqbal Hossain
Associate Professor
Department of CSE, Brac University

Cryptanalysis

- Cryptography - study of encryption principles/methods.
- Cryptanalysis (code breaking) - study of principles/methods of deciphering ciphertext without knowing key.
- Cryptographic systems are generically classified along three independent dimensions.

How to attack

- Brute force attack
- Cryptanalysis

Cryptanalysis

The type of operations used for transforming plaintext to ciphertext.

1.1 Substitution:

- Each element (bit, letter, group of bits or letters) in the plaintext is mapped into another element.

1.2 Transposition:

- Elements in the plaintext are rearranged.
- Fundamental requirement is that no information be lost.
- Product systems involve multiple stages of substitutions and transpositions.

Cryptanalysis

2. The number of keys used.

- Referred to as symmetric, single-key, secret-key, or conventional encryption if both sender and receiver use the same key.

- Referred to as asymmetric, two-key, or public-key encryption if the sender and receiver each use a different key.

Cryptanalysis

3. The way in which the plaintext is processed.

- A block cipher processes the input one block of elements at a time, producing an output block for each input block.
- A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

Cryptanalysis

Cryptanalysis

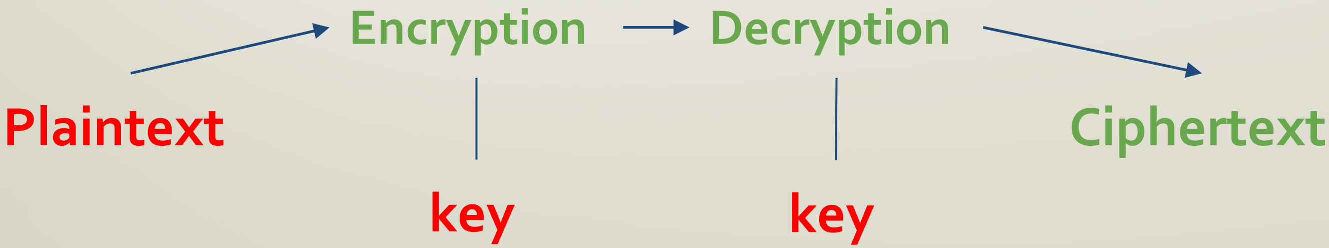
The strategy used by the cryptanalyst depends on the nature of the encryption scheme and the information available to the cryptanalyst.

- Cipher text Only
- Known Plaintext
- Chosen-plaintext
- Chosen-Cipher text

Cryptanalysis

1. Ciphertext Only:

- The cryptanalyst knows ciphertext only.
- Uses brute-force approach - try all possible keys.
- Make the key space very large so it becomes impractical.
- Easiest to defend



Encryption Decryption

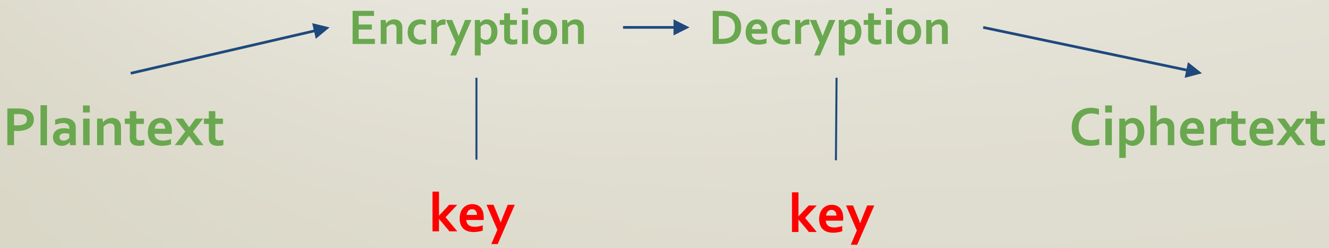
Plaintext Ciphertext

key key

Cryptanalysis

2. Known plaintext:

- The analyst may be able to capture one or more plaintext messages as well as their encryptions.
- Or he may know that certain plaintext patterns will appear in a message.
- May deduce the key.



Plaintext

Encryption

Decryption

Ciphertext

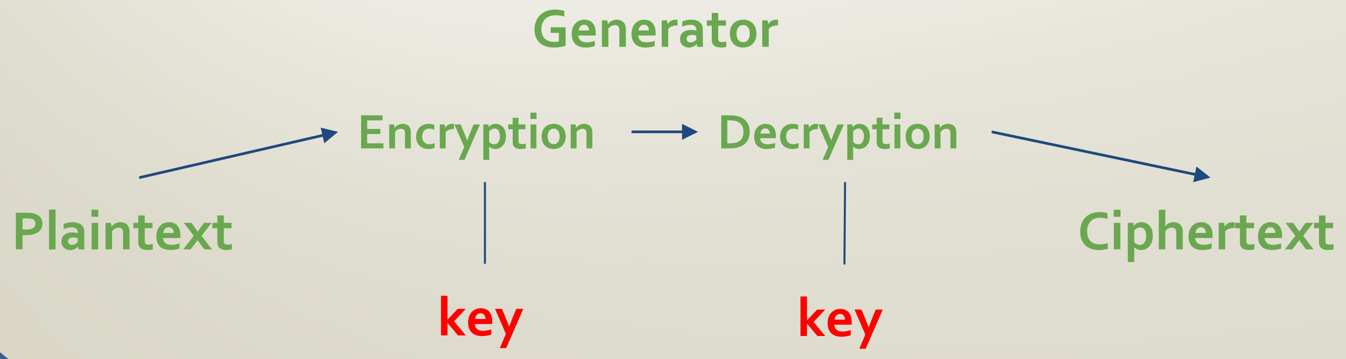
key

key

Cryptanalysis

3. Chosen-plaintext:

- A cryptanalyst can choose arbitrary plaintext data to be encrypted and then he receives the corresponding ciphertext.
- If the analyst is able to choose the messages to encrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.



Generator

Plaintext

Encryption

key

Decryption

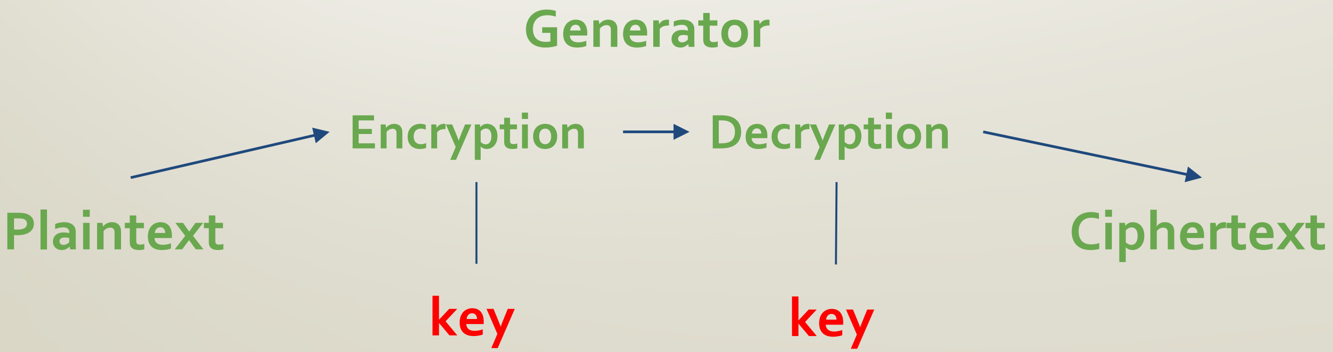
key

Ciphertext

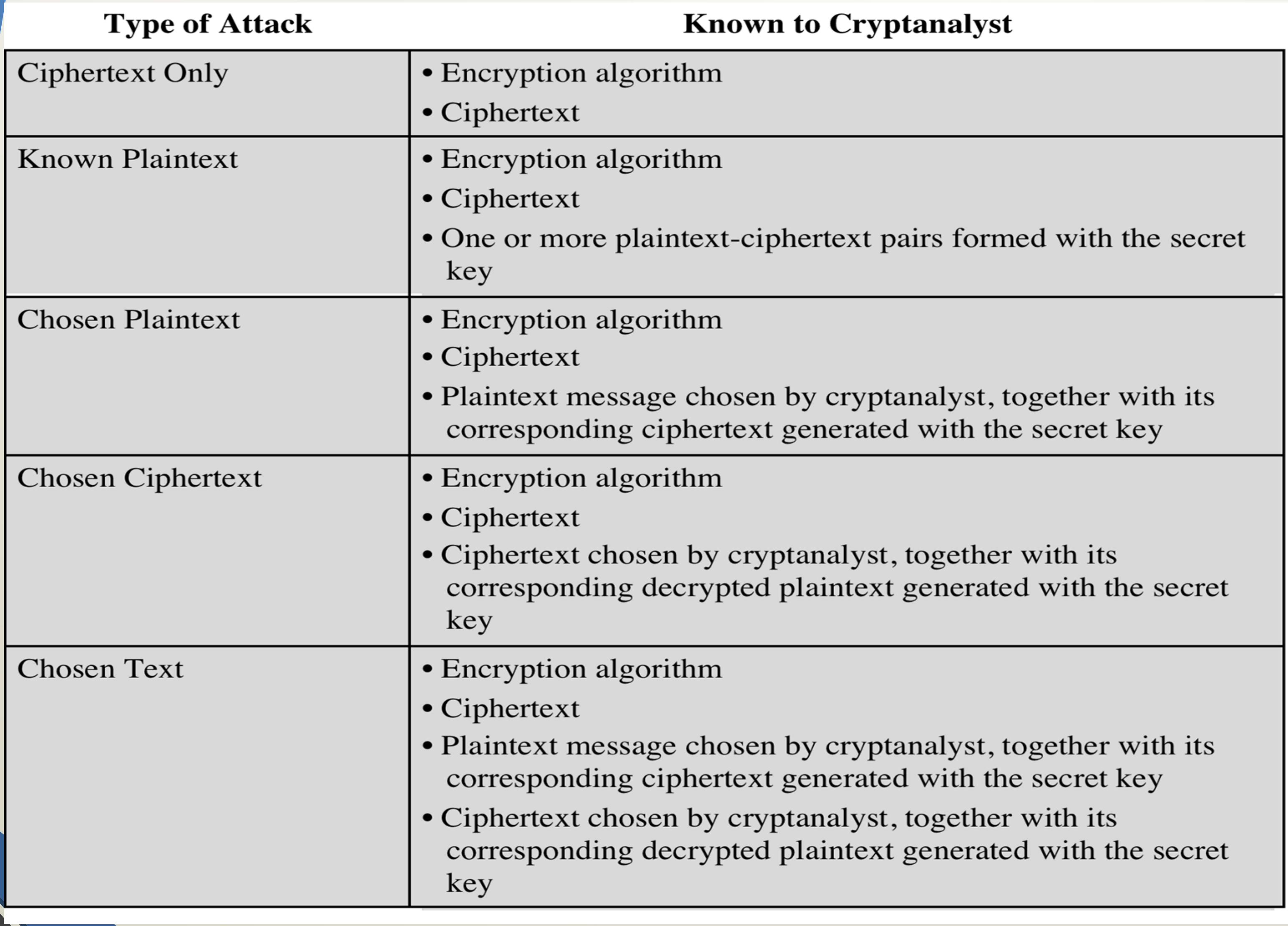
Cryptanalysis

4. Chosen-Ciphertext:

- a cryptanalyst can analyse any chosen ciphertexts together with their corresponding plaintexts
- If the analyst is able to choose the messages to decrypt, the analyst may deliberately pick patterns that can be expected to reveal the structure of the key.
- used for breaking systems with public key encryption



Cryptanalysis



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 • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Cryptanalysis

- Chosen ciphertext and chosen text are less commonly employed as cryptanalytic techniques but are nevertheless possible avenues of attack.
- Only a relatively weak algorithm will fail to withstand a ciphertext-only attack.
- Generally, an encryption algorithm is designed to withstand a **known-plaintext attack.**
- An encryption scheme is **computationally secure** if ciphertext generated by the scheme meets one or both of the criteria:
- The cost of breaking the cipher exceeds the value of the encrypted information.
- The time required to break the cipher exceeds the useful lifetime of the information.

Cryptanalysis

Brute Force attack:

- Involves trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success.
- Suppose that a cipher has a 100 bit key
  - Then keyspace is of size 2^{100}
- On average, for exhaustive search Trudy tests $2^{100}/2 = 2^{99}$ keys
- Suppose Trudy can test 2^{30} keys/second
  - Then she can find the key in about **37.4 trillion years**

Why Study Cryptanalysis?

- Study of cryptanalysis gives insight into all aspects of crypto
- Also gain insight into attacker’s mindset
  - “black hat” vs “white hat” mentality
- Cryptanalysis is more fun than cryptography
  - Cryptographers are boring
  - Cryptanalysts are cool
- But cryptanalysis is hard