Chapter 20

Symmetric Encryption and Message Confidentiality

Symmetric Encryption

- Also referred to as:
  - Conventional encryption
  - Secret-key or single-key encryption
- Only alternative before public-key encryption in 1970's
  - Still most widely used alternative
- Has five ingredients:
  - Plaintext
  - Encryption algorithm
  - Secret key
  - Ciphertext
  - Decryption algorithm

Cryptography

- classified along three independent dimensions:
  - The type of operations used for transforming plaintext to ciphertext
    - Substitution – each element in the plaintext is mapped into another element
    - Transposition – elements in plaintext are rearranged
  - The number of keys used
    - Sender and receiver use same key – symmetric
    - Sender and receiver each use a different key - asymmetric
  - The way in which the plaintext is processed
    - Block cipher – processes input one block of elements at a time
    - Stream cipher – processes the input elements continuously

Substitution Ciphers

- Replaces one symbol with another. If the symbols in the plaintext are alphabetic characters, we replace one character with another.

i

A substitution cipher replaces one symbol with another.

The simplest substitution cipher is a shift cipher (additive cipher)

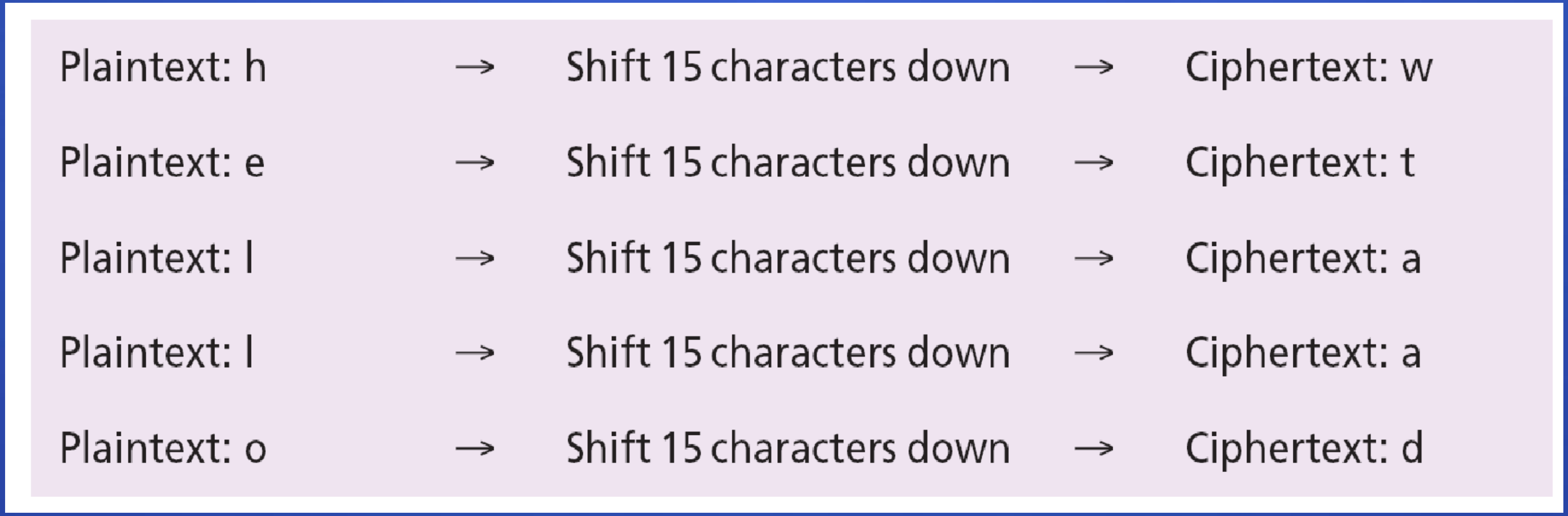
Substitution Cipher

Example Shift Cipher

- Use the additive cipher with key = 15 to encrypt the message “hello”.

Solution

- We apply the encryption algorithm to the plaintext, character by character:



Plaintext: h	→	Shift 15 characters down	→	Ciphertext: w
Plaintext: e	→	Shift 15 characters down	→	Ciphertext: t
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: l	→	Shift 15 characters down	→	Ciphertext: a
Plaintext: o	→	Shift 15 characters down	→	Ciphertext: d

- The ciphertext is therefore “wtaad”.

Transposition Ciphers

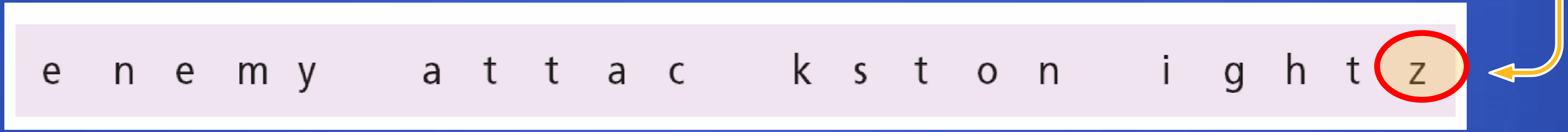
- A transposition cipher does not substitute one symbol for another, instead it changes the location of the symbols.
- A symbol in the 1st position of the *plaintext* may appear in the 10th position of the *ciphertext*, while a symbol in the 8th position in the *plaintext* may appear in the 1st position of the *ciphertext*.
- In other words, a transposition cipher reorders (transposes) the symbols.

i

A transposition cipher reorders symbols.

Transposition Cipher

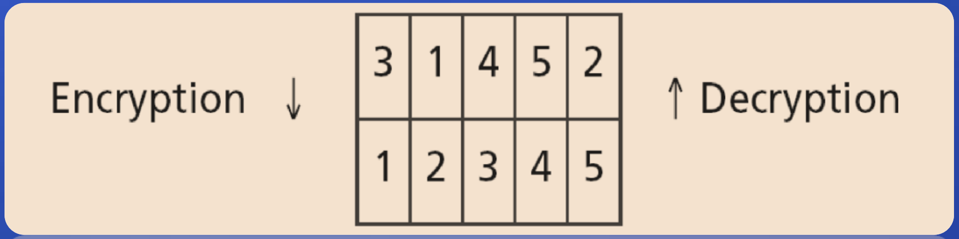
- Alice needs to send the message “*Enemy attacks tonight*” to Bob.
- Alice and Bob have agreed to divide the text into groups of five characters and then permute the characters in each group.
- The following shows the grouping after adding a bogus character (z) at the end to make the last group the same size as the others.



enemy attac kston ightz

The key used for encryption and decryption is a permutation key, which shows how the character are permuted.

For this message, assume that Alice and Bob used the following key:



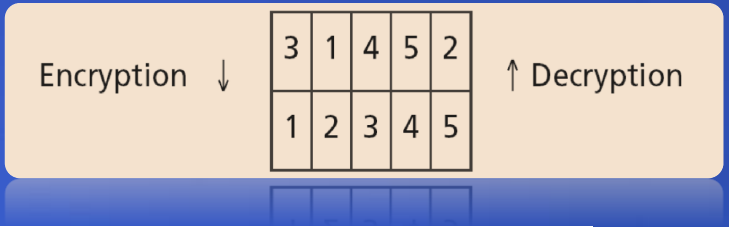
Encryption ↓

3	1	4	5	2
1	2	3	4	5

↑ Decryption

Transposition Cipher

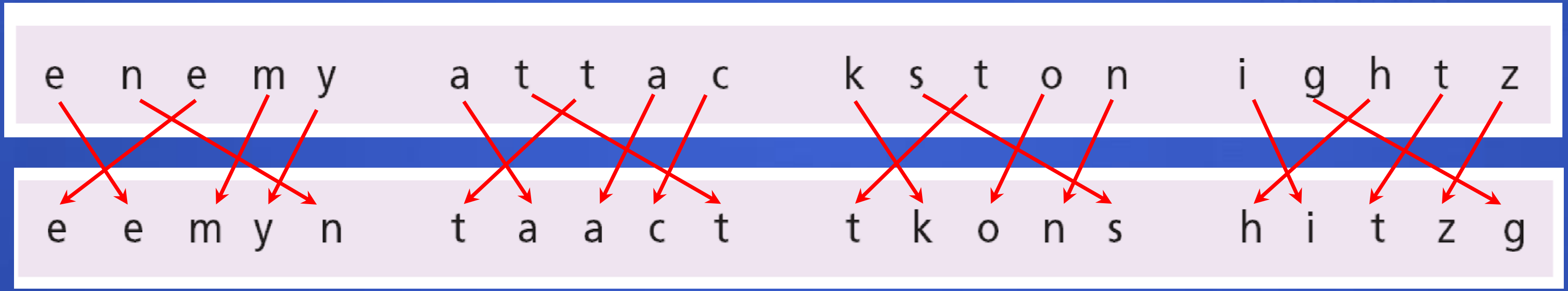
- The 3rd character in the *plaintext* block becomes the 1st character in the *ciphertext* block. Etc….
- The permutation yields:



Encryption ↓

3	1	4	5	2
1	2	3	4	5

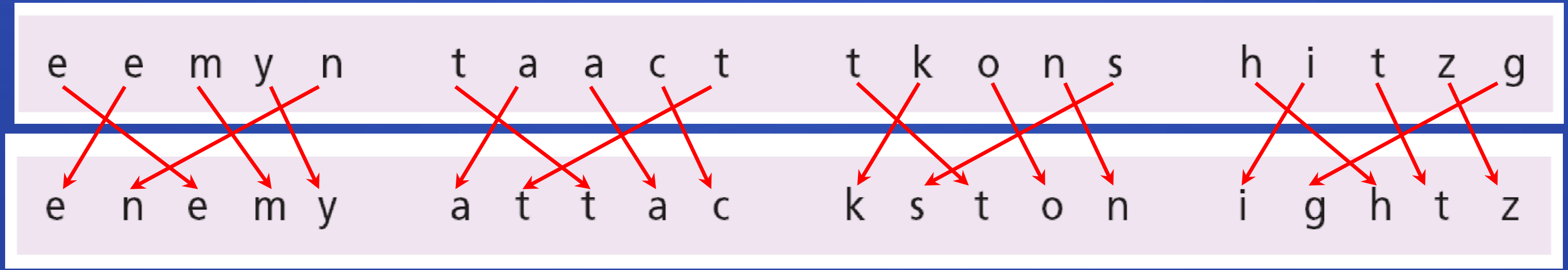
↑ Decryption



e n e m y a t t a c k s t o n i g h t z

e e m y n t a a c t t k o n s h i t z g

- Alice sends the *ciphertext* "eemyntaacttkonshitzg" to Bob.
- Bob divides the *ciphertext* into five-character groups and, using the key in the reverse order, finds the *plaintext*.



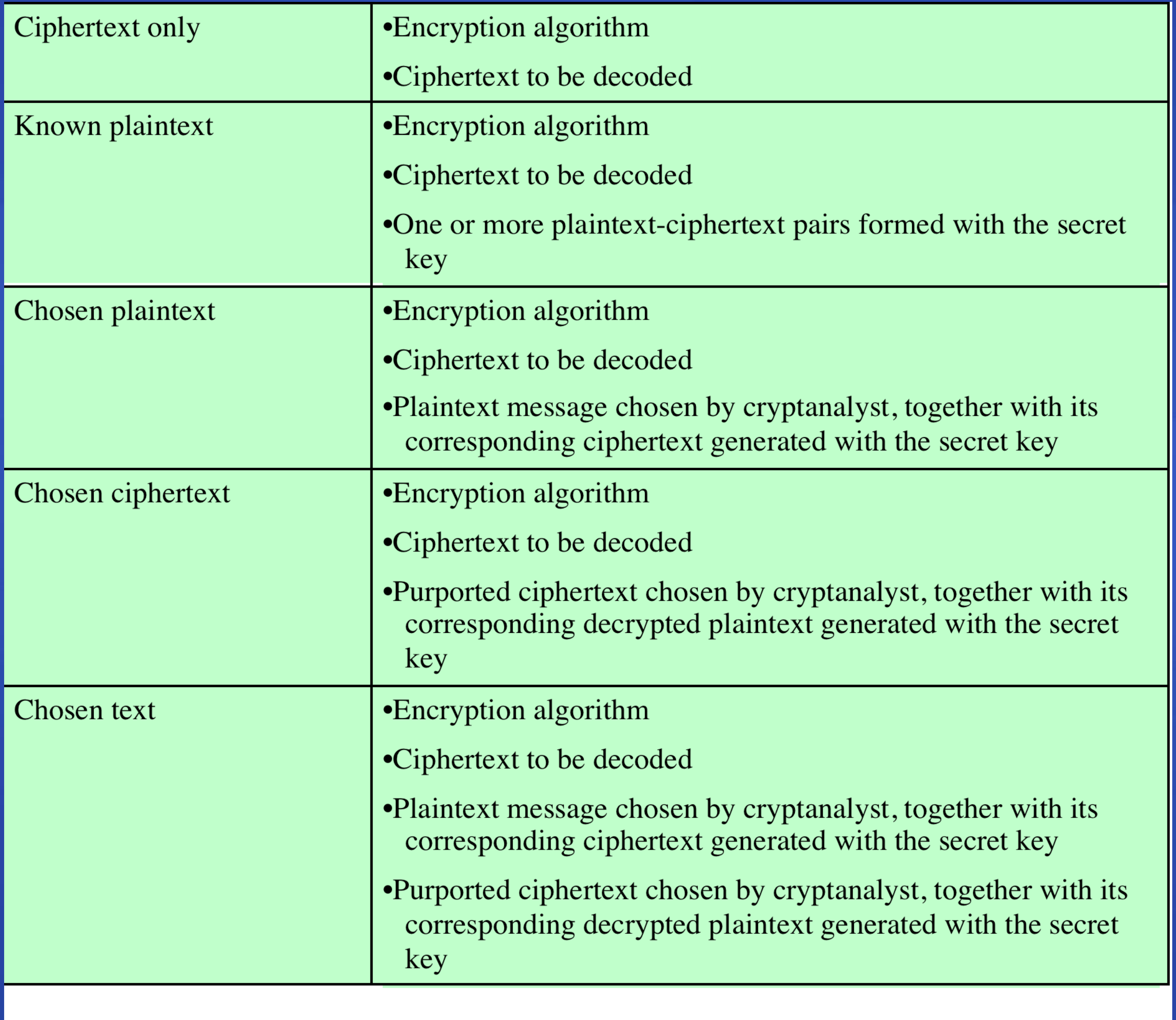
e e m y n t a a c t t k o n s h i t z g

e n e m y a t t a c k s t o n i g h t z

Symmetric (Secret Key) Encryption

- Since these traditional ciphers are no longer secure due to PC processing power, modern symmetric-key ciphers have been developed over the last few decades.
- Modern ciphers normally use a combination of substitution, transposition and some other complex transformations to create a *ciphertext* from a *plaintext*.
- Modern ciphers are bit-oriented (instead of character-oriented). The *plaintext*, *ciphertext* and the *key* are strings of bits.
- Some examples of modern symmetric-key ciphers are DES, AES and IDEA.

Cryptanalysis



type of attack	known to cryptanalyst
Ciphertext only	•Encryption algorithm •Ciphertext to be decoded
Known plaintext	•Encryption algorithm •Ciphertext to be decoded •One or more plaintext-ciphertext pairs formed with the secret key
Chosen plaintext	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen ciphertext	•Encryption algorithm •Ciphertext to be decoded •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen text	•Encryption algorithm •Ciphertext to be decoded •Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key •Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

Computationally Secure Encryption Schemes

- Encryption is computationally secure if:
  - Cost of breaking cipher exceeds value of information
  - Time required to break cipher exceeds the useful lifetime of the information
- Usually very difficult to estimate the amount of effort required to break
- Can estimate time/cost of a brute-force attack