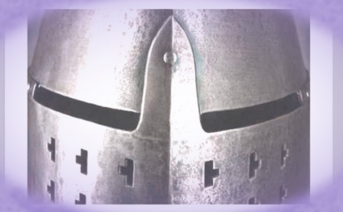


Cryptography and Network Security

Eighth Edition

by William Stallings

Chapter 3

Classical Encryption Techniques

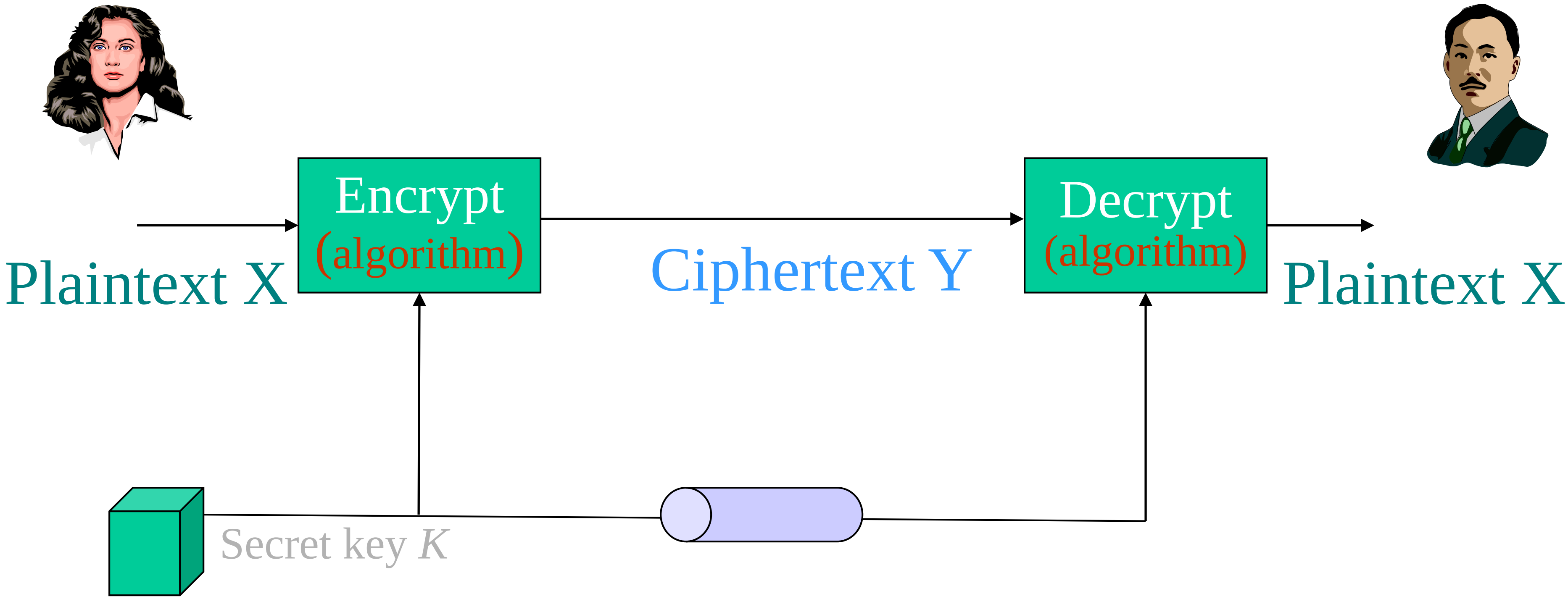
Basic Cryptography

- Private Key Cryptography
  - Secret Key Cryptography, Symmetric Cryptography, Classical Cryptography
- Public Key Cryptography

Brief History

- All encryption algorithms from BC till 1976 were secret key algorithms
  - Also called private key algorithms or symmetric key algorithms
  - Julius Caesar used a substitution cipher
  - Widespread use in World War II (enigma)
- Public key algorithms were introduced in 1976 by Whitfield Diffie and Martin Hellman

Classical Cryptography



Classical Cryptography

- Sender, receiver share common key
  - Keys may be the same, or trivial to derive from one another
  - Sometimes called *symmetric cryptography*
- Two basic types
  - Transposition ciphers
  - Substitution ciphers
- Product ciphers
  - Combinations of the two basic types

Cryptosystem

- Quintuple ($\mathcal{E}$, $\mathcal{D}$, $\mathcal{M}$, $\mathcal{K}$, $\mathcal{C}$)
  - $\mathcal{M}$ set of plaintexts
  - $\mathcal{K}$ set of keys
  - $\mathcal{C}$ set of ciphertexts
  - $\mathcal{E}$ set of encryption functions E: $\mathcal{M} \times \mathcal{K} \to \mathcal{C}$
  - $\mathcal{D}$ set of decryption functions D: $\mathcal{C} \times \mathcal{K} \to \mathcal{M}$

Classical Cryptography

- $c = E_k(m)$: Ciphertext ← Encryption
- $m = D_k(c)$: Plaintext ← Decryption
- k = encryption and decryption key
- The functions $E_k()$ and $D_k()$ must be inverses of one another
  - $E_k(D_k(c)) = ?$
  - $D_k(E_k(m)) = ?$
  - $E_k(D_k(m)) = ?$

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Example: Cæsar cipher
  - $\mathcal{M}$ = { sequences of letters }
  - $\mathcal{K} = \{ k \mid k$ is an integer and $0 \leq k \leq 25 \}$
  - $\mathcal{E} = \{ E_k \mid k \in \mathcal{K}$ and for all letters m,

    $E_k(m) = (m + k) \bmod 26 \}$
  - $\mathcal{D} = \{ D_k \mid k \in \mathcal{K}$ and for all letters c,

    $D_k(c) = (26 + c - k) \bmod 26 \}$
  - $\mathcal{C} = \mathcal{M}$

Cæsar cipher

Let k = 9, m = "VELVET" (21 4 11 21 4 19)

$E_k(m)$ = (21+9 4+9 11+9 21+9 4+9 19+9) mod 26

= (30 13 20 30 13 28) mod 26

="4 13 20 4 13 2" = "ENUENC"

$D_k(m)$ = (26 + c – k) mod 26

= (21 30 37 21 30 19) mod 26

= "21 4 11 21 4 19" = "VELVET"

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Substitution Ciphers

- Cæsar cipher is a substitution cipher.
- Substitution Cipher: Change characters in plaintext to produce ciphertext
- Example (Cæsar cipher)
  - Plaintext is `HELLO WORLD;`
  - Key is 3, usually can be written as letter ‘D’
  - Ciphertext is `KHOOR ZRUOG`

Vigenère Cipher

- Like Cæsar cipher, but use a phrase as the key
- Example
  - Message `THE BOY HAS THE TOY`
  - Key `VIG`
  - Encipher using Cæsar cipher for each letter:

key	`VIGVIGVIGVIGVIG`
plain	`THEBOYHASTHETOY`
cipher	`OPKWWECIYOPKOWE`

Discussion: how to implement Vigenère Cipher?

- What is your design consideration, speed or storage space?
- What kind of functions are you going to use?

Use look-up Table to Encipher

	G	*I*	*V*
A	G	I	V
B	H	J	W
E	K	M	Z
H	N	P	C
O	U	W	J
S	Y	A	N
T	Z	B	O
Y	E	H	T

- Table on the left with relevant rows, columns only
- key letters on top, plaintext letters on the left
- Example encipherments:
  - key V, letter T: follow V column down to T row (giving "O")
  - Key I, letter H: follow I column down to H row (giving "P")

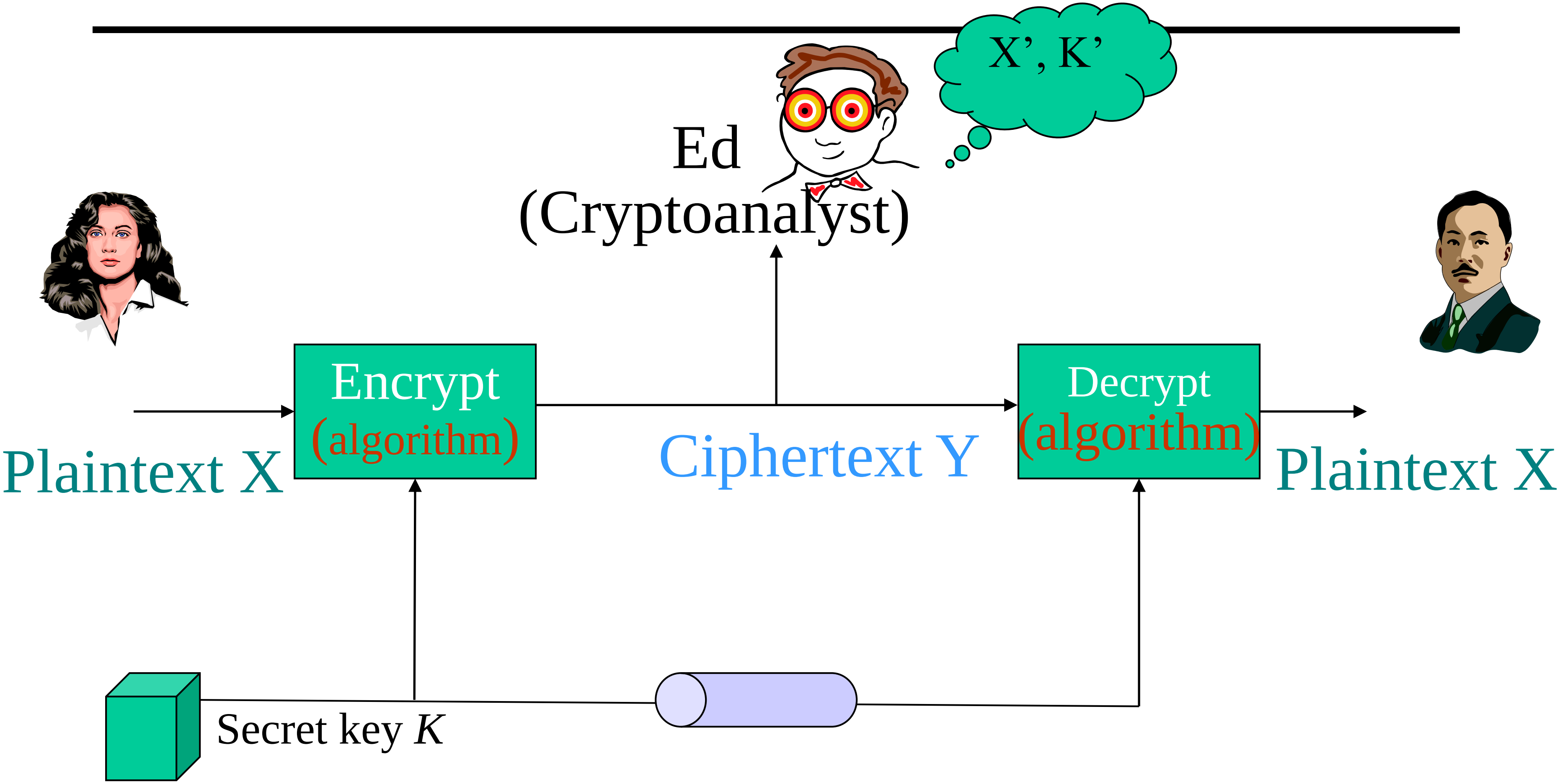
Transposition Cipher

- Rearrange letters in plaintext to produce ciphertext
- Example (Rail-Fence Cipher)
  - Plaintext is `HELLO WORLD`
  - Rearrange as

    ```
    HLOOL
    ELWRD
    ```

  - Ciphertext is `HLOOL ELWRD`

Classical Cryptography – Possible Attacks



Discussion: How to attack Cæsar cipher?

Let k = 9, m = "VELVET" (21 4 11 21 4 19)

$E_k(m)$ = (21+9 4+9 11+9 21+9 4+9 19+9) mod 26

= (30 13 20 30 13 28) mod 26

="4 13 20 4 13 2" = "ENUENC"

$D_k(m)$ = (26 + c – k) mod 26

= (21 30 37 21 30 19) mod 26

= "21 4 11 21 4 19" = "VELVET"

Attacks

- Opponent whose goal is to break cryptosystem is the *adversary*
- Three types of attacks:
  - ***ciphertext only***: adversary has only ciphertext; goal is to find plaintext, possibly key
  - ***known plaintext***: adversary has ciphertext, corresponding plaintext; goal is to find the key
  - ***chosen plaintext***: adversary may supply plaintexts and obtain corresponding ciphertext; goal is to find key

Attacking a conventional cryptosystem

- Cryptoanalysis:
  - Art/Science of breaking an encryption scheme
  - Exploits the characteristics of algorithm/ mathematics
    - Recover plaintext from the ciphertext
    - Recover a key that can be used to break many ciphertexts
- Brute force
  - Tries all possible keys on a piece of ciphertext
    - If the *number of keys* is small, the adversary can get the correct key easily by simply trying!

Crack Caesar Cipher!

- example:

  Plaintext: ?

  Key : ?

  Ciphertext: `PHHW PH DIWHU WKH WRJD SDUWB`

- Try all possible keys: 0, 1, 2, … 25.
- It works when key=`3`: meaningful plaintext generated.
- We are done!

How about more complicated ciphers?

- Mono-alphabetic substitution cipher
  - Each plaintext letter is randomly assigned to its ciphertext letter.

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**
q	**a**	**z**	**w**	**s**	**x**	**e**	**d**	**c**	**r**	**f**	**v**	**t**	**g**	**b**	**y**	**h**	**n**	**u**	**j**	**m**	**i**	**k**	**o**	**l**	**p**

  - How many possible ways of assignment?
    - 26!
    - Takes a looooong time to try every possible assignment.

Basis for Cryptoanalysis

- Mathematical attacks
  - Based on analysis of underlying mathematics
- Statistical attacks
  - Make assumptions about the distribution of letters, pairs of letters, triplets of letters, *etc*. (called models of the language).
  - Examine ciphertext, correlate properties with the assumptions.

Statistical Attacks Example

- Rail-Fence Cipher
  - Plaintext is `HELLO WORLD`
  - Rearrange as

    ```
    HLOOL
    ELWRD
    ```
  - Ciphertext is `HLOOL ELWRD`

Attacking the Cipher

- Anagramming
  - If 1-gram frequencies match English frequencies, but other *n*-gram frequencies do not,
  - Then probably a transposition
  - Rearrange letters to form *n*-grams with highest frequencies

Example

- Ciphertext: `HLOOLELWRD`
- Frequencies of 2-grams beginning with H
  - HE 0.0305
  - HO 0.0043
  - HL, HW, HR, HD < 0.0010
- Frequencies of 2-grams ending in H
  - WH 0.0026
  - EH, LH, OH, RH, DH ≤ 0.0002
- Implies E may follow H

Example

- Arrange so that H and E are adjacent

```
HE
LL
OW
OR
LD
```

- Read off across, then down, to get original plaintext

Summary

- Present an overview of the main concepts of symmetric cryptography
- Explain the difference between cryptanalysis and brute-force attack
- Understand the operation of Ceaser cipher and attacks

- Transposition cipher v.s. Substitution cipher
- Brute-force attack v.s. Cryptoanalysis
- Understand the operation of Vigenère Cipher