Fundamentals of Cybersecurity

Chapter Three: Cryptography

Senait Desalegn

School of Information Technology and Engineering
Addis Ababa Institute of Technology
Addis Ababa University
March 2024

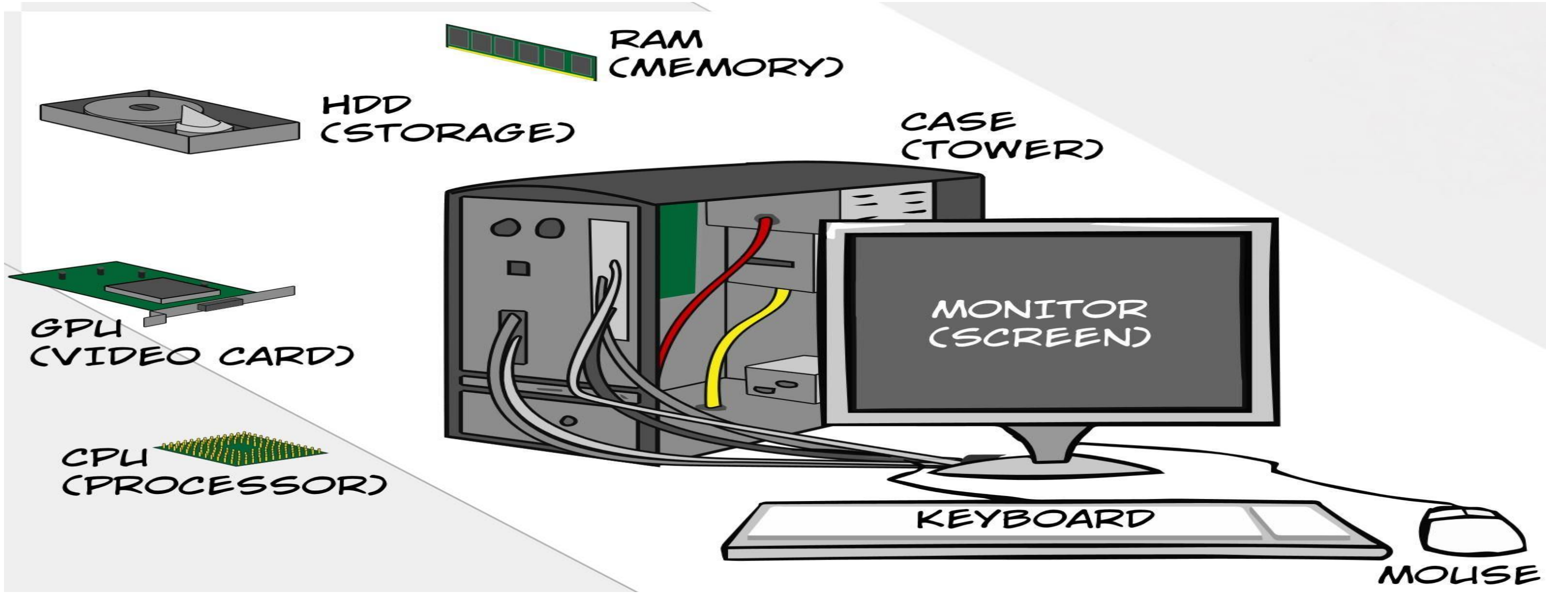
Contents

CHAPTER 3

Application and OS security

A Computer Model

An operating system has to deal with the fact that a computer is made up of a **CPU**, **random access memory** (RAM), **input/output** (I/O) devices, and long-term **storage**.



OS Concepts

An **operating system (OS)** provides the **interface between** the **users** of a computer and that computer's **hardware**.

An operating system **manages** the ways **applications access** the resources in a computer, including its **disk drives**, **CPU**, **main memory**, **input devices**, **output devices**, and **network interfaces**.

- An operating system **manages multiple users**.
  - Unique **needs** and **rights** of **users/groups** should be **respected /malicious** activities **avoided**
- An operating system **manages multiple programs**.
  - Protecting each **running** app from **interfering** with **each other**/ avoid damaging of **resources** by **malicious** apps

Basic Terminologies

- **Cryptanalysis -** deals with finding the encryption key without the knowledge of the encryptor
- **Cryptology -** deals with cryptography and cryptanalysis
- **Cryptanalysis** – deals with breaking (cracking) encryption
- **Cryptosystems -** are computer systems used to encrypt data for secure transmission and storage
- **Cipher -** is a method for encrypting messages
- **Plaintext -** is text that is in readable form
- **Ciphertext -** results from plaintext by applying the encryption key

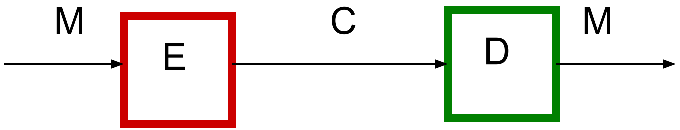
Basic Terminologies…

- **Keys -** are rules used in algorithms to convert a document into a secret document
- Keys are of two types:
  - Symmetric
    - the same key is used both for encryption and decryption
    - E.g. DES (Data Encryption Standard), AES (Advanced En. St.)
  - Asymmetric
    - different keys are used for encryption and decryption
    - E.g. RSA (Rivest-Shamir-Adleman)

Basic Terminologies…

- Basic Notations
  - M message,
  - P plaintext
  - C ciphertext,
  - E encryption,
  - D decryption,
  - k key

- $C = E(M)$
- $C = E(M, k)$
- $M = D(C)$
- $M = D(C, k)$

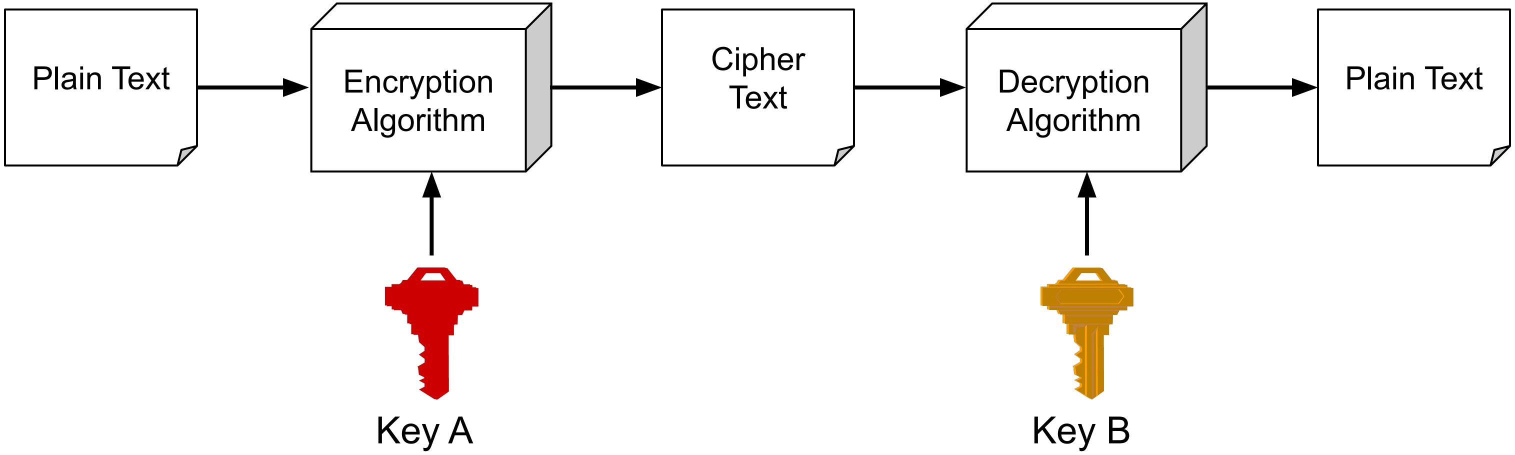


Encryption Techniques

Kerckhoffs's Principle

- An encryption scheme should be secure even if enemy knows everything about it except the key
  - Attacker knows all algorithms
  - Attacker does not know random numbers
    - use a good random number generator!
- Secret algorithm creates additional hurdle
  - Hard to keep secret if used widely
- Do not rely on secrecy of the algorithms
  - "security by obscurity"

Encryption

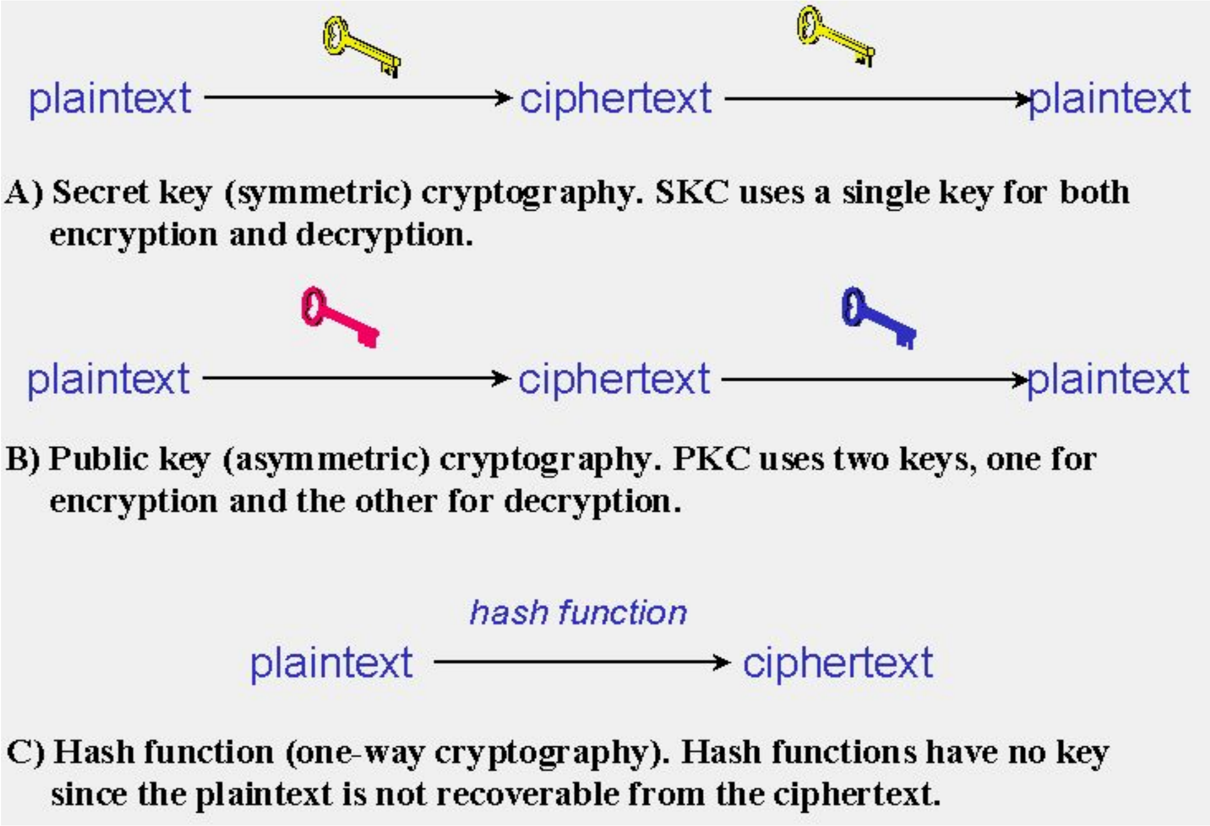


- Encryption algorithms are standardized & published
- The key which is an input to the algorithm is secret

Types of cryptographic algorithms

- Encryption and decryption are conducted using algorithms
- Cryptographic algorithms can be classified based on the number of keys that are employed for encryption and decryption.
- The three types of algorithms:
  - Secret Key Cryptography (SKC): Uses a single key (symmetric key) for both encryption and decryption
  - Public Key Cryptography (PKC): Uses one key for encryption and another for decryption (asymmetric key)
  - Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information

Types of cryptographic algorithms…



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

C) Hash function (one-way cryptography). Hash functions have no key since the plaintext is not recoverable from the ciphertext.

Secret Key Cryptography (Symmetric)

- A single key is used for both encryption and decryption.
- The sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver.
- The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext.
- Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.
- With this form of cryptography, it is obvious that the key must be known to both the sender and the receiver; that, in fact, is the secret.
- The biggest difficulty with this approach is the distribution of the key.

Public-Key Cryptography (Asymmetric)

- Generic Public-Key Cryptography (PKC(employs two keys
  - One key to encrypt the plaintext and the other key to decrypt the ciphertext.
- The two keys are mathematically related
- Knowledge of one key does not allow to easily determine the other key.
- Because a pair of keys are required for the process to work, this approach is also called **asymmetric cryptography**.
- One of the keys is designated the public key and may be advertised as widely as the owner wants.
- The other key is designated the private key and is never revealed to another party.

Hash functions

- **Hash functions**, also called **message digests** and **one-way encryption**, are algorithms that use no key
  - Instead, a fixed-length hash value is computed based upon the plaintext
  - impossible for either the contents or length of the plaintext to be recovered.
- Hash algorithms are typically used to provide a digital fingerprint of a file's contents,
  - often used to ensure that the file has not been altered by an intruder or virus (provide a measure of the integrity of a file)
  - commonly employed by many operating systems to encrypt passwords.
- E.g: Message Digest (MD) algorithms

Symmetric Cryptography

Classical Symmetric cryptography

Classical Ciphers

- Classical crypto techniques have been around since the early ages.
  - Two major techniques
    - Substitution – replace one letter with another
    - Transposition – change the position of letters in predefined way

- Current crypto techniques use a product cipher
  - combination of the two

Caesar Cipher

- Earliest known substitution cipher
  - Substitution replaces one basic unit (letter/byte) with another
  - Substitution is one of the fundamentals of modern crypto systems
  - Julius Caesar replaced each letter by 3rd letter for military communication

```
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
                         ↓
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

- Example:

```
meet me after the class
PHHW PH DIWHU WKH FODVV
```

Caesar Cipher

- Define transformation as:

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
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- Mathematically give each letter a number

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

- Then have Caesar cipher as:

$$C = \mathrm{E}(p) = (p + k) \bmod (26)$$

$$p = \mathrm{D}(\mathrm{C}) = ((\mathrm{C} - k) + 26) \bmod (26)$$

Caesar Cipher…

- Violates “no security through obscurity”
- Only have 25 possible ciphers
  - A maps to B,..Z
- How will you attack this crypto system?
  - E.g., break ciphertext "GCUA VQ DTGCM“
  - Given ciphertext, just try all shifts of letters (There can only be 26? (25) possible keys)
- Do need to recognize when have plaintext and stop there
  - Easy for humans hard and for computers
  - What if the message was in, say, Amharic?

Monoalphabetic Cipher

- Key size of Caesars cipher was small
  - Allowed brute-force attack
- Rather than shifting the alphabet we could *shuffle* (jumble) the letters arbitrarily
  - Each plaintext letter maps to a different random ciphertext letter

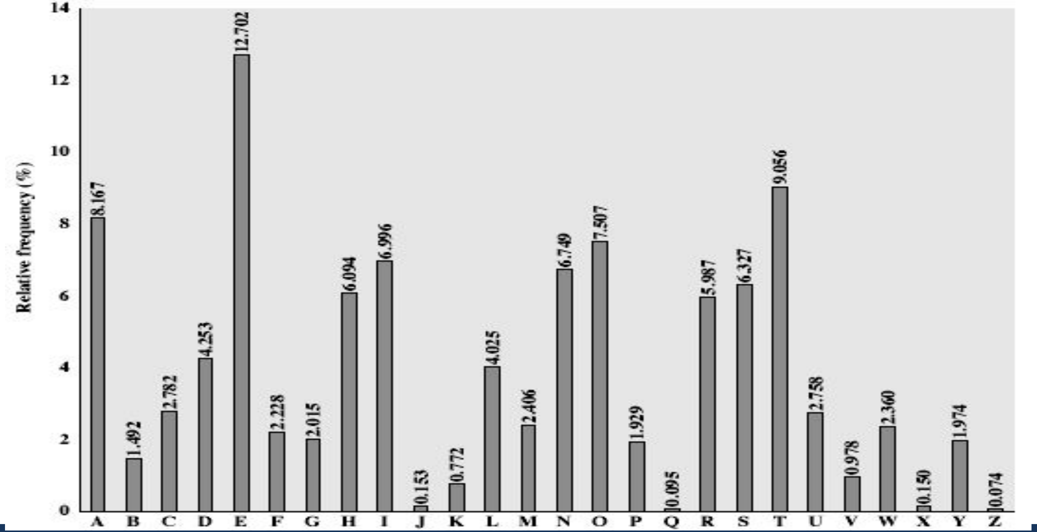
```
Plain:   abcdefghijklmnopqrstuvwxyz
Key:     DKVQFIBJWPESCXHTMYAUOLRGZN
Plaintext:  ifwewishtoreplaceletters
Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA
```

- Key is 26 letters long
  - Now have a total of 26! = 4 x 10^{26} keys
  - Try 1 key per µsec … 10 trillion years

Monoalphabetic Cipher…

- Problem with this crypto is language characteristics
  - Human languages are **redundant**
  - Letters are not equally commonly used

E	12.31%	L	4.03%	B	1.62%
T	9.59	D	3.65	G	1.61
A	8.05	C	3.20	V	0.93
O	7.94	U	3.10	K	0.52
N	7.19	P	2.29	Q	0.20
I	7.18	F	2.28	X	0.20
S	6.59	M	2.25	J	0.10
R	6.03	W	2.03	Z	0.09
H	5.14	Y	1.88		



Monoalphabetic Cipher…

- Given ciphertext:

  UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBME
  TSXAIZVUEPHZHMDZSHZOWSFPAPPDTSVPQUZWYMX
  UZUHSXEPYEPOPDZSZUFPOMBZWPFUPZHMDJUDTMOHM
  Q

P 13.33	H 5.83	F 3.33	B 1.67	C 0.00
Z 11.67	D 5.00	W 3.33	G 1.67	K 0.00
S 8.33	E 5.00	Q 2.50	Y 1.67	L 0.00
U 8.33	V 4.17	T 2.50	I 0.83	N 0.00
O 7.50	X 4.17	A 1.67	J 0.83	R 0.00
M 6.67				

E 12.31%	**L** 4.03%	**B** 1.62%
T 9.59	**D** 3.65	**G** 1.61
A 8.05	**C** 3.20	**V** 0.93
O 7.94	**U** 3.10	**K** 0.52
N 7.19	**P** 2.29	**Q** 0.20
I 7.18	**F** 2.28	**X** 0.20
S 6.59	**M** 2.25	**J** 0.10
R 6.03	**W** 2.03	**Z** 0.09
H 5.14	**Y** 1.88	

Monoalphabetic Cipher…

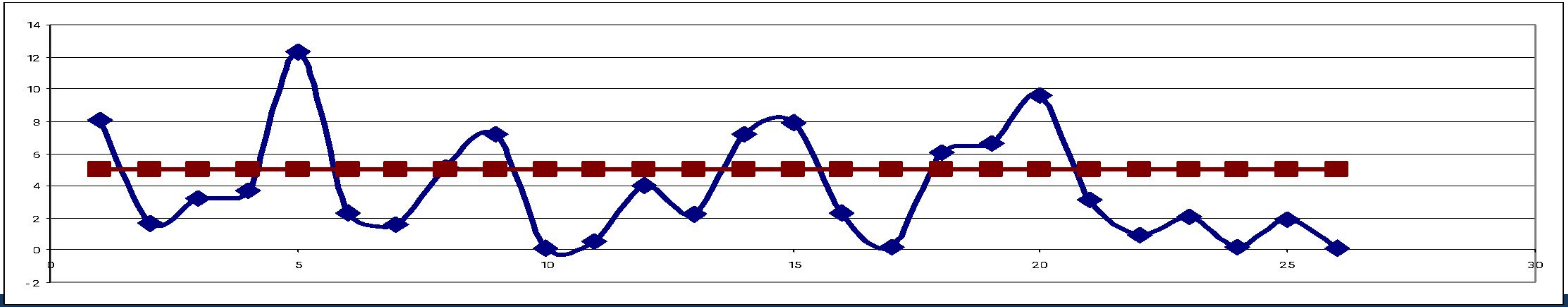
- Count relative letter frequencies (see text)
  - Guess P & Z are e and t
  - Guess ZW is th and hence ZWP is the –th (using two and three latter frequency distribution tables)

- Proceeding with trial and error finally get:

```
it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow
```

Monoalphabetic Cipher…

- Problems with monoalphabetic ciphers
  - Frequency of letters in ciphertext reflects frequency of plaintext
- Want a single plaintext letter to map to multiple ciphertext letters
  - “e” → “x”, “c”, “w”
- Ideally, ciphertext frequencies should be flat



Polyalphabetic Substitutions

- Pick k substitution ciphers
  - $\pi_1\ \pi_2\ \pi_3\ \ldots\ \pi_k$
  - Encrypt the message by rotating through the k substitutions

m	e	s	s	a	g	e
$\pi_1(\mathbf{m})$	$\pi_2(\mathbf{e})$	$\pi_3(\mathbf{s})$	$\pi_4(\mathbf{s})$	$\pi_1(\mathbf{a})$	$\pi_2(\mathbf{g})$	$\pi_3(\mathbf{e})$
q	**a**	**x**	**o**	**a**	**u**	**v**

- Same letter can be mapped to multiple different ciphertexts
  - Helps smooth out the frequency distributions

Vigenère Tableau

- Multiple substitutions
  - Can choose “complimentary” ciphers so that the frequency distribution flattens out
  - More generally: more substitutions means flatter distribution
- Vigenère Tableau
  - Collection of 26 permutations
    - 26 possible substitutions
  - Usually thought of as a 26 x 26 grid
  - Key is a word

Vigenère Tableau

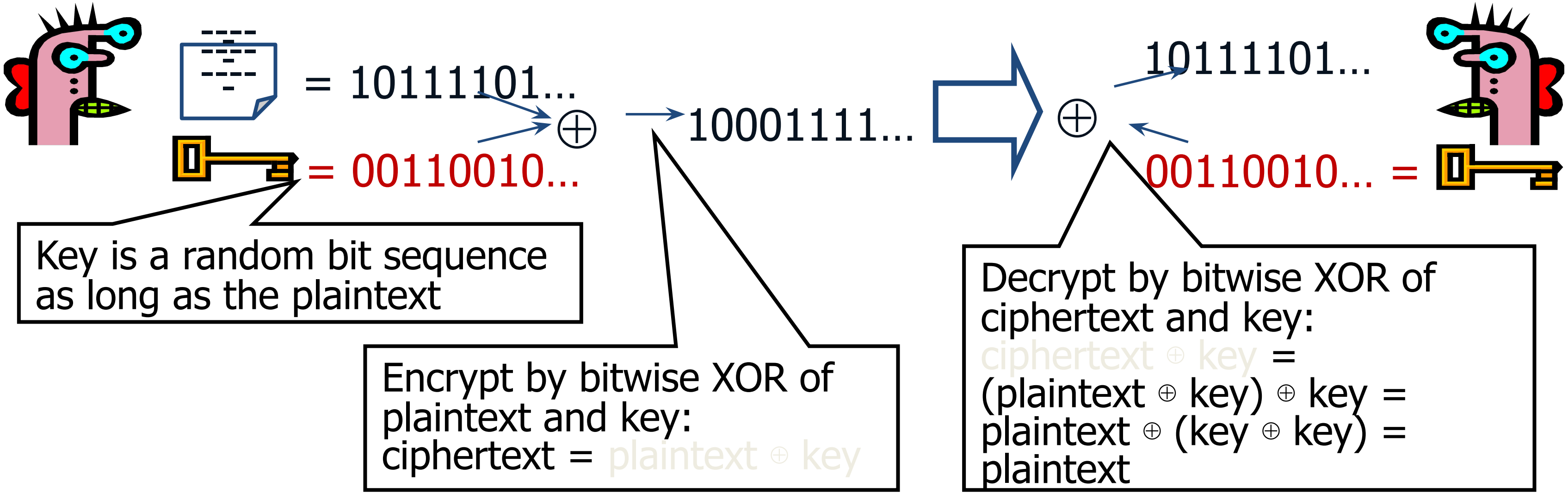
	a	b	c	d	e	f	g	.	.	.
A	a	b	c	d	e	f	g	.	.	.
B	b	c	d	e	f	g	h	.	.	.
C	c	d	e	f	g	h	i	.	.	.
D	d	e	f	g	h	i	j	.	.	.
E	e	f	g	h	i	j	k	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.

Plaintext: a bad deed

Key "bed": B EDB EDBE

Ciphertext: b fde hgfh

One-Time Pad (Ideal Cipher)



- Cipher achieves perfect secrecy if and only if there are as many possible keys as possible plaintexts, and every key is equally likely
  - E.g., a random sequence of 0's and 1's XORed to plaintext, no repetition of keys

One-Time Pad (ideal cipher)

- Unbreakable since ciphertext bears no statistical relationship to the plaintext
  - For **any** plaintext, it needs a random key of the same length
    - Hard to generate large amount of keys
- Have problem of safe distribution of key
- Current systems have adopted the XOR operation but not the key length

Advantages of One-Time Pad

- Easy to compute
  - Encryption and decryption are the same operation
  - Bitwise XOR is very cheap to compute
- As secure as theoretically possible
  - Given a ciphertext, all plaintexts are equally likely, regardless of attacker's computational resources
  - …if and only if the key sequence is truly random
    - True randomness is expensive to obtain in large quantities
  - …if and only if each key is as long as the plaintext
    - But how do the sender and the receiver communicate the key to each other? Where do they store the key?

Problems with One-Time Pad

- Key must be as long as the plaintext
  - Impractical in most realistic scenarios
  - Still used for diplomatic and intelligence traffic
- Does not guarantee integrity
  - One-time pad only guarantees confidentiality
  - Attacker cannot recover plaintext, but can easily change it to something else
- Insecure if keys are reused
  - Attacker can obtain XOR of plaintexts

Symmetric Cryptography

Modern Symmetric cryptography

Thank you!