

# Information Communication Technologies

## Lecture 14. Security Technologies

Kassymova Aizhan Bakhytzhonovna

PhD, Associate professor

[a.kassymova@satbayev.university](mailto:a.kassymova@satbayev.university)

# Agenda

1 Encryption

2 Applications of Encryption

3 Authentication



# Encryption

- **Encryption** is the process of transforming information so it is unintelligible to eavesdroppers
- **Decryption** is the process of transforming encrypted information so that it is intelligible to the intended recipient



# Encryption

- Communication via secret code has a long history, dating back at least to the ancient Greeks.
- **Cryptography algorithms** are mathematical functions used for encryption or decryption
- **DES** (Data Encryption Standard) – for electronic commerce
- **RC4** (from RSA Security, Inc) – for Internet applications





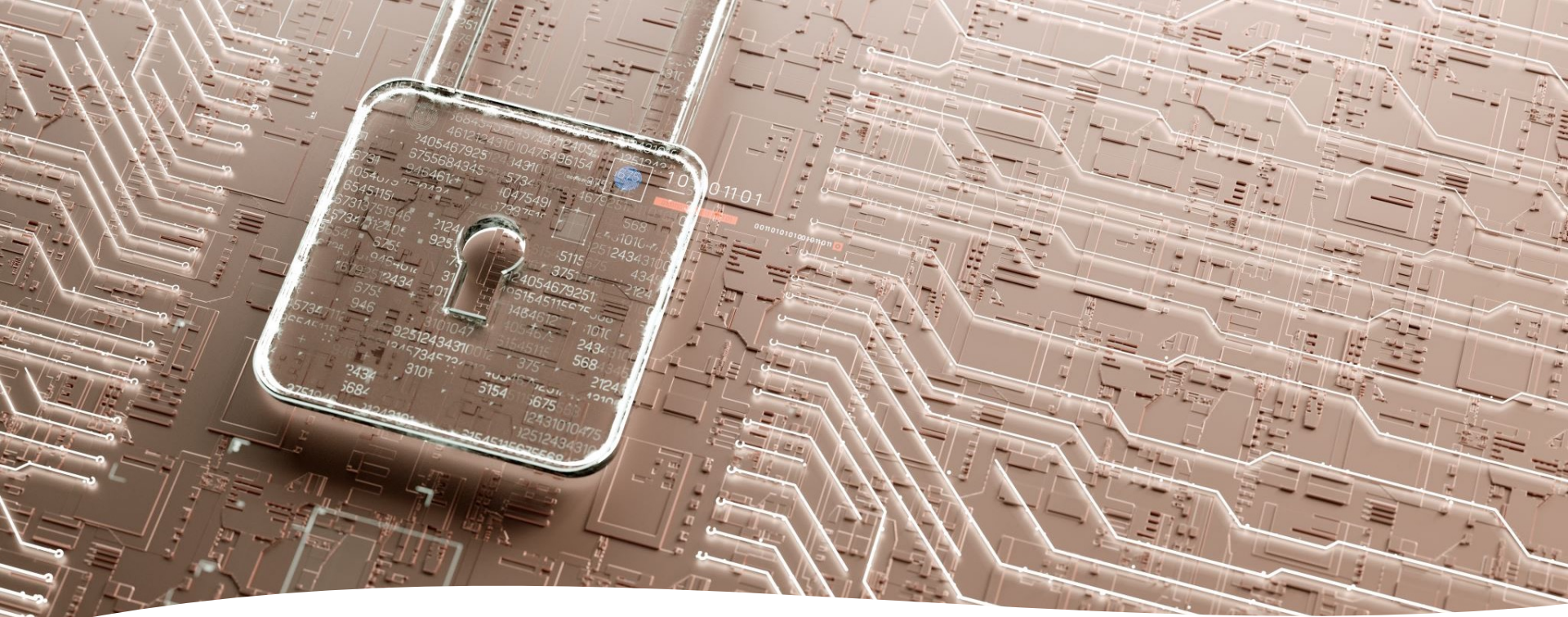
# Encryption Terminologies

- **Plaintext** – original message to be encrypted
- **Ciphertext** – encrypted version of message
- **Private key** – a scheme that uses the same key to encrypt and decrypt messages
- **Public key** – a scheme that uses one key to encrypt and another key to decrypt messages
- **Keyspace** – the size and complexity of the encryption scheme
- **Brute force attack** – method of trying to break the code of a small keyspace scheme by using all possible combinations

# Encryption

- A **substitution cipher** changes the plaintext to ciphertext by replacing each element of the plaintext with its encrypted substitute.

Message	Encryption Technique	Encrypted Message
HELLO WORLD	shift right by one character	IFMMP XPSME
IBM	shift left by one character	HAL

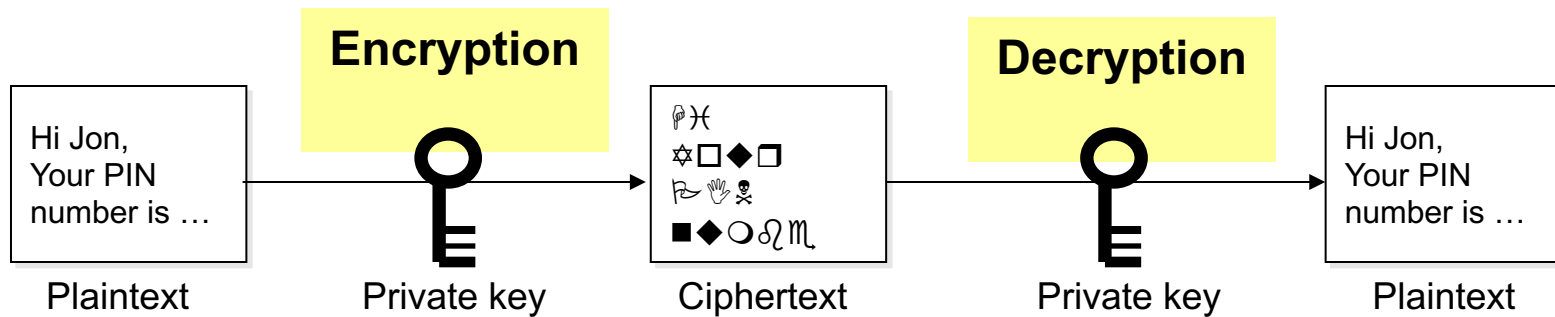


# Encryption

- **Encryption** is the process of scrambling or hiding information so that it cannot be understood until it is decrypted.
- Scrambling and unscrambling data requires a **key (secret code)**
  - One popular public key encryption systems is called **Pretty Good Privacy** or **PGP**
  - Two main types of encryption:
    - Private-key encryption (symmetric encryption)
    - Public-key encryption (asymmetric encryption)

# Private Key Encryption

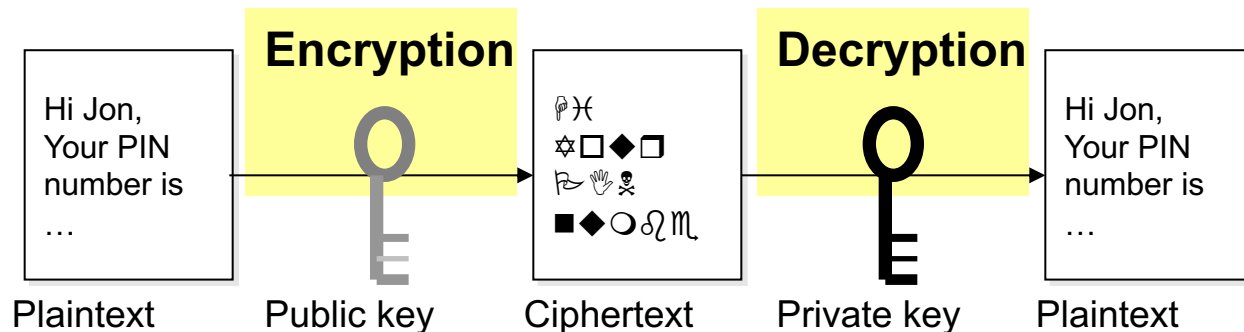
- Same key is used by the sender to encrypt and the receiver to decrypt a message.
- Key is only known to the sender and the recipient.





# Public Key Encryption

- Uses two keys
  - Public key (known to everyone)
    - Encrypts the message
  - Private key (known to the recipient)
    - Decrypts the message
- Requires a lot of computation, so it is slower than other types of codes (**number theory**).
- Calculations required to break a code might take way too long—perhaps trillions of years, even on a very fast computer.





# Hybrid Encryption Scheme

- Uses public key encryption to send a freshly-created key, called the *session key*.
- Encrypt the actual message using a symmetric encryption scheme like **RC4** or **DES**, based on the session key.
- Because **session keys are generated randomly** and **thrown away after one use**, eavesdropper will be unable to decrypt any other messages between the same parties
- Reasonably secure
- Takes advantage of the efficiency of the simpler symmetric encryption schemes.

# Applications of Encryption

- **Email**
- **Hard Drives** (The intruder can make a copy of the hard drive, a process known as **mirroring**, and thus steal the data it contained)
- **DVD Movies** (scheme called CSS (Content Scrambling System))
- **Cellular Phones**





# Authentication

- ***Authentication*** is the process of confirming an identity, determining whether you are who you claim to be.





# Good Passwords

- Difficult to guess
- At least 8 characters long, the longer the better (if you can remember it)
- Contains a mix of uppercase letters, lowercase letters, numbers, symbols, and punctuation marks
- Characters are arranged in an unpredictable order
- Can be typed in quickly by you to prevent someone from obtaining your password by looking at your key strokes



# Bad Passwords

- Based on personal information such as all or part of your name, nickname, birth date, company name, and relative's name
- Based on surrounding objects, such as "computer", "desk", "book" or words from a dictionary
- Names of fictional characters from movies or books
- Words spelled in a particular patten (e.g. with the last letter omitted, backwards)
- Character sequence that is easy to type, such as "asfd" and "qwer"
- Characters that follow a certain pattern such as "abcabcdabcde" and "1122334455"
- Passwords you have seen or used previously



# Generating Good Passwords

- Use a password generator application
- Use the third letter of each word (more than 2 characters long) from a randomly selected sentence  
Example:
  - Sentence: "AUTHENTICATION is the process of confirming an identity, determining whether someone is who he claims to be."
  - Password: "Teonetemoa."
- Insert symbols randomly (e.g. "Te\*netem\$a.")
- Mix of uppercase letters, lowercase letterers, numbers, symbols, and punctuation marks (e.g. "T1e\*netEm\$a.")

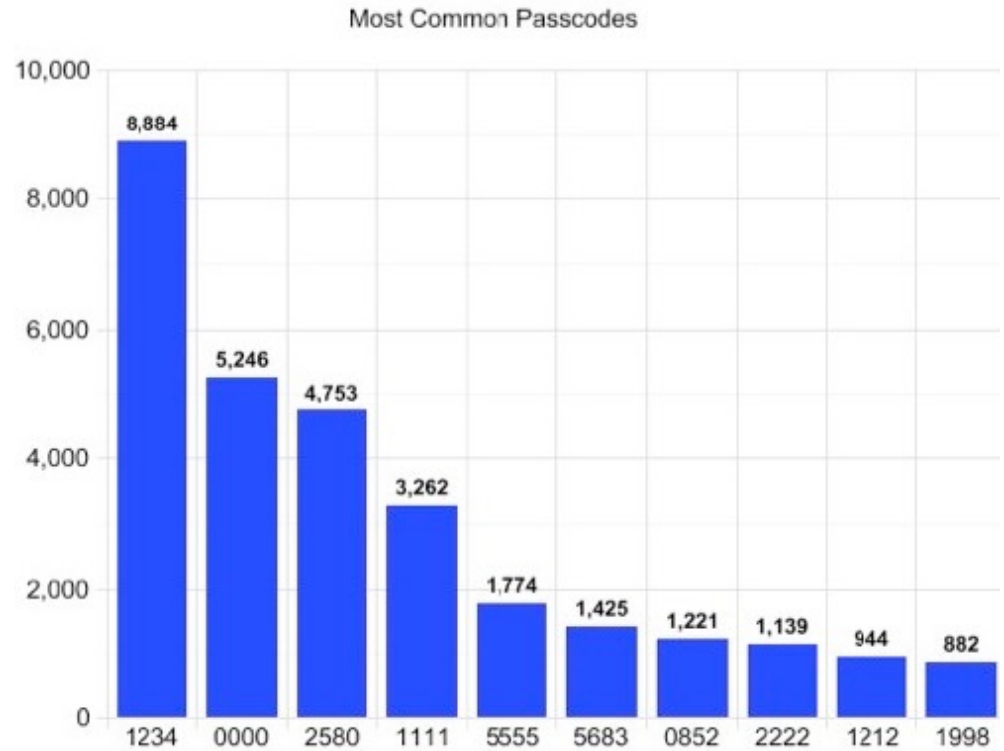


# Most popular internet passwords

- 1. 123456
- 2. 12345
- 3. 123456789
- 4. Password
- 5. iloveyou
- 6. princess
- 7. rockyou
- 8. 1234567
- 9. 12345678

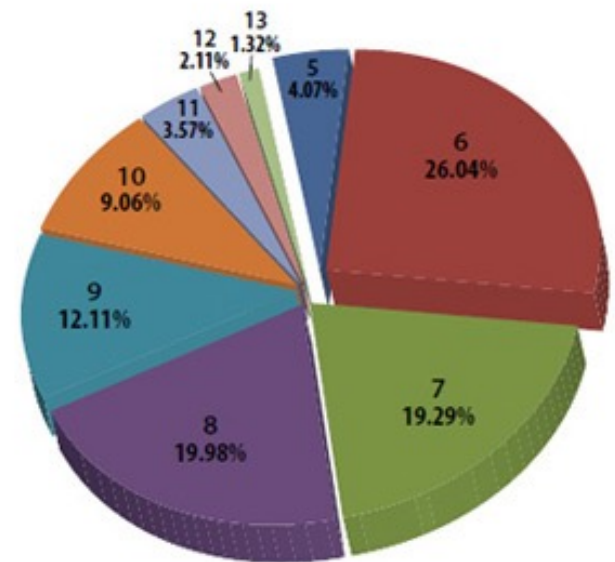


Most  
popular  
iPhone  
passwords



# Passwords

Password Length Distribution





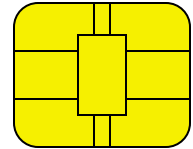
# TOP passwords in vKontakte

- 123456 134 0,34%
- qwerty 85 0,21%
- 111111 51 0,13%
- 1234567890 41 0,10%
- 123321 34 0,09%
- 666666 33 0,08%
- 1234567 31 0,08%
- 123123 29 0,07%
- 12345678 26 0,07%
- qwertyuiop 26 0,07%
- qazwsxedc 25 0,06%
- 000000 23 0,06%
- любовь 23 0,06%
- 555555 22 0,06%
- zxcvbnm 22 0,06%
- 654321 19 0,05%
- gfghjkm 19 0,05%
- 1q2w3e4r 18 0,05%

# Smart Cards

- Credit card-sized plastic card with an embedded integrated circuit chip that can serve as a secure medium for storing personal identification information such as

- picture identifications
- voiceprints
- fingerprints,
- signatures
- account information.



- Chip consists of a **microprocessor, ROM, RAM, and electrically erasable programmable read only memory (EEPROM)**.
- EEPROM enables the chip to retain its state even when power is removed.





# Smart Cards

- Information on card can be read by a custom-programmed reader for authentication
- Can be used as an access key to a computer system
- Can be embedded on phone cards, banking cards or health cards
- Contain security features such as data encryption
- Self-containment of a smart card allows it to be resistant to network or Internet attacks.

# Biometrics

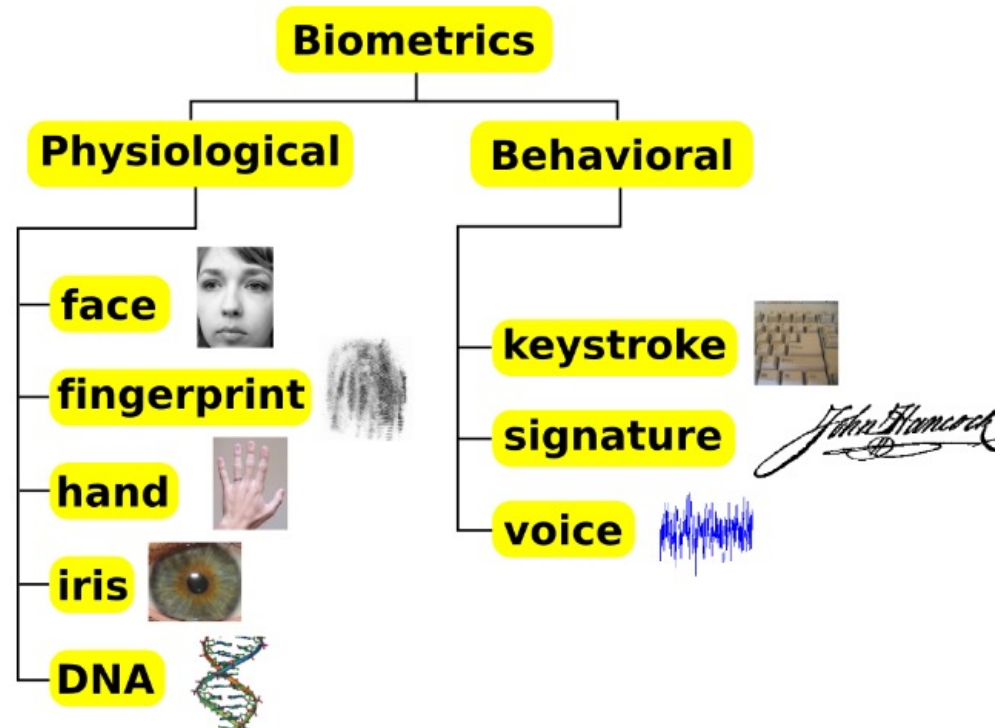
- **Automatic identification of a person based on his/her physiological or behavioral characteristics**


- facial features
- fingerprints
- handwriting
- iris
- voice



- More secure than traditional methods because the person is required to be present at the point-of-identification.

# Biometrics





## Biometrics (continued)

- Don't need to remember passwords or PINs, or carry identification cards
- Prevent unauthorized access to or fraudulent use of ATMs, cellular phones, smart cards, desktop PCs, workstations, and computer networks
- Used by governments, military divisions, electronic banking, law enforcement, and social services



# Biometrics Example: Fingerprint Scanner

Fingerprint scanners can confirm your identity in less than two seconds.





# Digital Signatures

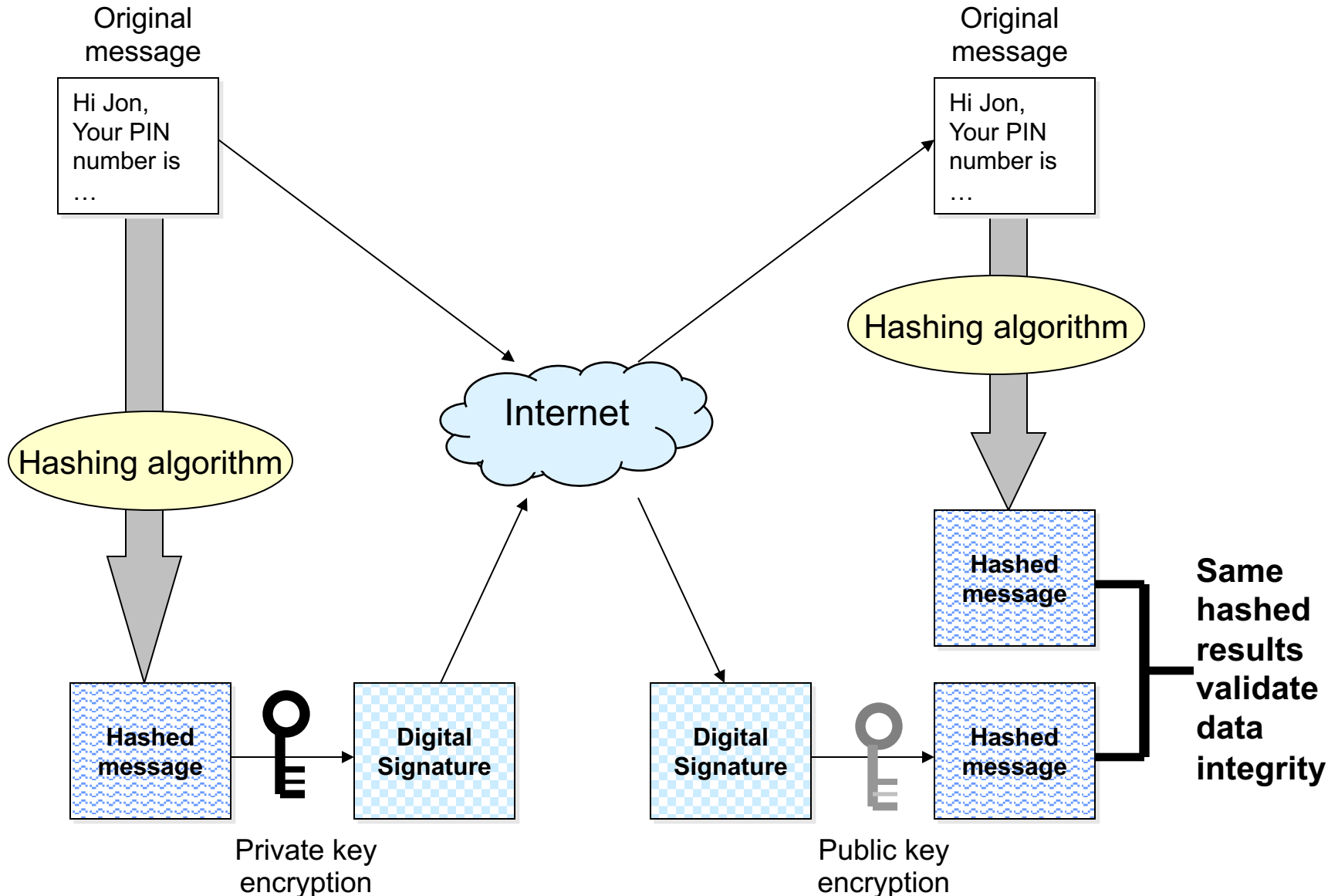
- Can be used as proof that a message originated from the sender
- Must be both unique to the sender and unique to the particular message so that it can be verified but not reused
- Needs to create a "hash code" for the plaintext message
- A ***hash code*** is a numerical value computed from the plaintext in such a way that any change to the plaintext, even to just one character, will cause the hash code to change as well.



## Digital Signatures (continued)

- Uses public key encryption, public-key and private-key pairs.
- Variation from encrypting messages, to generate digital signatures, sender uses the private key to encrypt the hash of the message to indicate that the message did originate from the sender, and the receiver would decrypt that data with the sender's public key.
- Message is genuine because only the sender has the private key to encrypt the data.


# Generating and Verifying a Digital Signature





# Steps for Generating and Verifying a Digital Signature

- Sender:
  1. Transform the entire message using a hashing algorithm to generate a hash of the message.
  2. Generate the digital signature by encrypting the message hashed using the sender's private key.



# Steps for Generating and Verifying a Digital Signature (continued)

- Receiver:
  1. Transform the entire message using a hashing algorithm to generate a hash of the message.
  2. Decrypt the digital signature using the sender's public key.
  3. Compare the message hashed, and the decrypted digital signature. If these two hashes are the same, then the receiver can trust that the message was sent from the sender and that the message was not altered during transmission.



# Digital Certificate and Certificate Authority

- ***Digital certificate*** is an electronic identity document whose purpose is to help prevent impersonation.
- A ***certificate authority (CA)*** is a trusted third-party organization or company that validates identities and issues certificates.
- Certificates are used to associate public keys with entities (e.g. organizations, people).

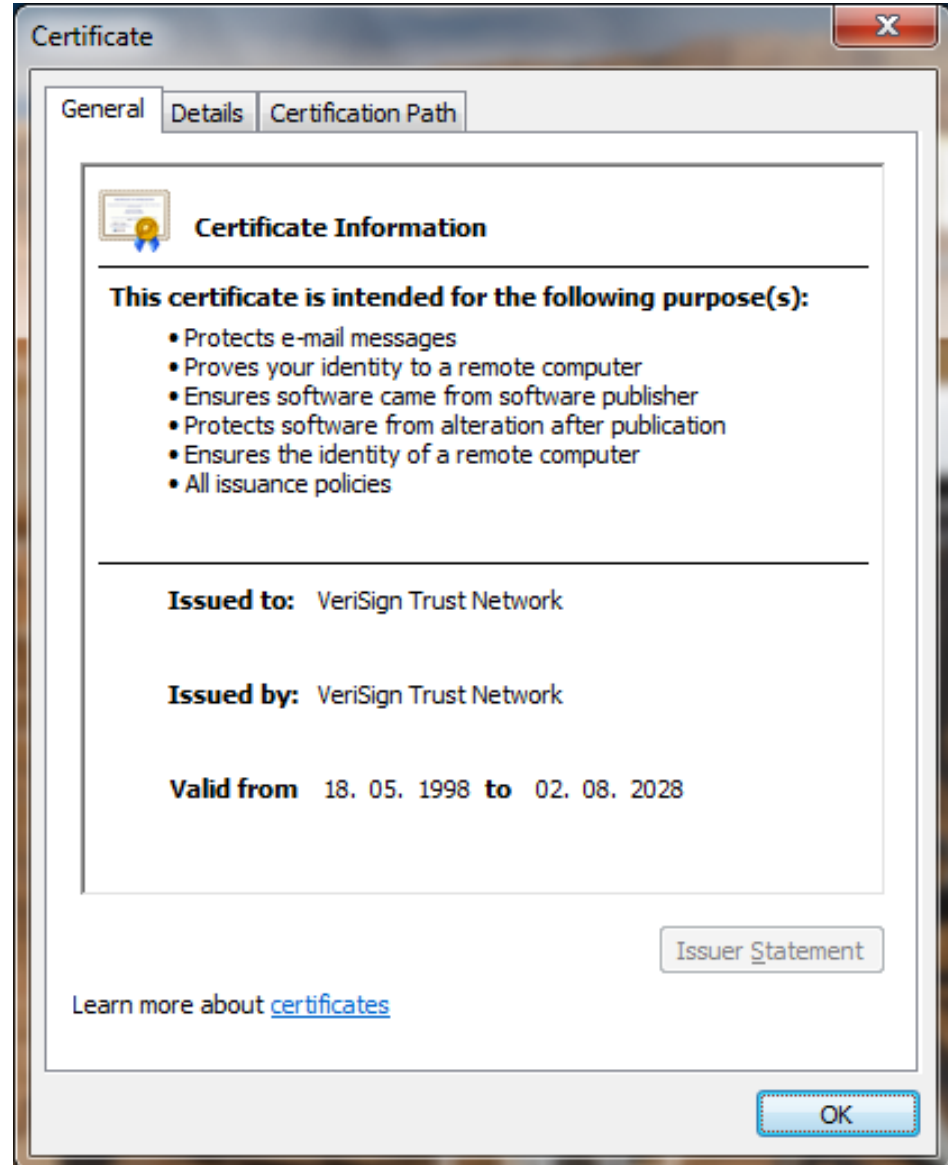


# Digital Certificate and Certificate Authority

- Before issuing a certificate, the CA must verify the identity of the entity requesting for the certificate.
- The certificate issued by the CA associates a **specific public key** with the entity requesting for the certificate. .
- Certificate also includes **the name of the entity it identifies, an expiration date, the name of the CA that issued the certificate, and a serial number.**
- Most importantly, a certificate includes the **digital signature** of the issuing CA to ensure the authenticity of the certificate.




# Sample Digital Certificate





# SSL Protocol

- **SSL (Secure Socket Layer)** is a protocol layer.
  - Operates on top of TCP/IP to provide encrypted communications.
- The protocol is a set of rules governing
  - server authentication,
  - client authentication, and
  - encrypted communication between servers and clients.
- Widely used on the Internet, especially for interactions that involve exchanging confidential information such as credit card numbers

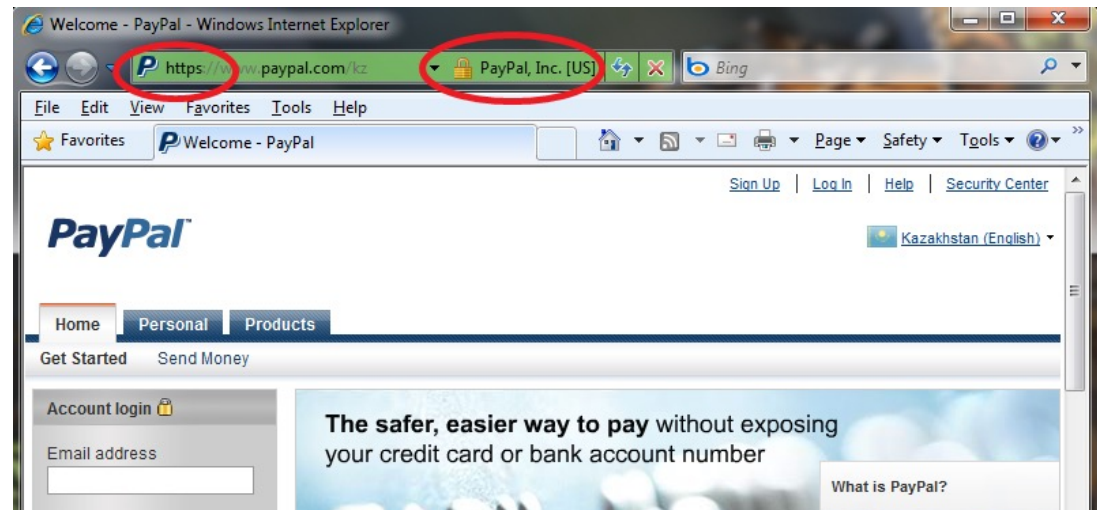


## SSL Protocol (continued)

- Uses public key cryptography to transmit a unique session key for each connection.
- It then uses a faster, symmetric encryption algorithm such as DES or RC4 to encrypt whatever information the application needs to transmit.
- To verify the identity of a Web server, e.g. [www.Amazon.com](http://www.Amazon.com), the SSL asks the server for its public key and it requires the key to be digitally signed by a certificate authority.

# Indications of an SSL Connection

- URL starts with **https** instead of **http**
- Lock icon appear at the right side of the address bar of the web page window
- SSL protocols encrypts data being transmitted



# SSL Protocol (continued)

## Encryption - why?



Expiry 09/08



Expiry 09/08

# SSL Protocol (continued)

## Encryption - how?



## SSL Protocol (continued)

### Encryption - how?

1. Computers agree on how to encrypt
2. Server sends certificate
3. Your computer says 'start encrypting'
4. The server says 'start encrypting'
5. All messages are now encrypted

# Encryption - how?

## I. Computers agree on how to encrypt



Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

Key	Cipher	Hash
RSA	RC4	HMAC-MD5
Diffie-Hellman	Triple DES	HMAC-SHA
DSA	AES	

Version	3.3
Random number	29873456234234...



# Encryption - how?

## 2. Server sends a certificate



Serial: 123123  
Issuer: Verisign  
Valid: from-to  
Public key  
Subject:  
Site  
Company  
Address

# Encryption - how?

3. Your computer says 'start encrypting'



Client Key  
Exchange

Both computers calculate a master secret code

Change  
Cipher Spec

Your computer is asking server to encrypt

Finished

Let's start now

# Encryption - how?

4. The server says 'start encrypting'



I'm going to send encrypted messages now



Let's go

Change  
Cipher Spec

Finished

# Encryption - how?

4. The server says 'start encrypting'



Change  
Cipher Spec

'f33^ v%p98

# Encryption - how?

5. All messages are now encrypted



hx&@HX373  
nwd73\*§dh'm  
/!\*yqw



# Encrypted Transactions

- ***Encrypted transactions*** ensure that credit card numbers cannot be intercepted between a computer and an e-commerce site.

During secure transactions, Internet Explorer, Firefox and Chrome displays a lock icon.



# Encrypted Transactions (continued)

The image shows a Windows Internet Explorer browser window displaying the PayPal website. The address bar shows the URL <https://www.paypal.com/kz>. A 'Certificate' dialog box is open, showing the following information:

**Website Identification**  
VeriSign Class 3 Public Primary CA has identified this site as:  
PayPal, Inc.  
San Jose, California  
US  
This connection to the server is encrypted.  
Should I trust this site?  
[View certificates](#)

**Certificate Information**  
**This certificate is intended for the following purpose(s):**  
• Ensures the identity of a remote computer  
  
\* Refer to the certification authority's statement for details.  
  
**Issued to:** www.paypal.com  
**Issued by:** VeriSign Class 3 Extended Validation SSL CA  
**Valid from:** 28. 04. 2009 **to:** 02. 04. 2010  
  
[Issuer Statement](#)  
  
[Learn more about certificates](#)

The background shows the PayPal website with a login form and a banner for 'The safer, easier way to pay with your credit card or bank account'.

End of Lecture 14