

Lecture 30-31

Ecommerce - Web Security

Mr. Mubashir Ali

Lecturer (Dept. of Computer Science)

dr.mubashirali1@gmail.com

Outline

- **Web security overview**
- **Secure transmission of data**
- **User's security issues**
- **Service provider's issues**

1. Web security

- Web client **expect** web applications to be **secure**
 - **preventing** access from untrusted or malicious sources to private data
 - service providers do not **misuse** their data
 - by **exchanging** data with third party

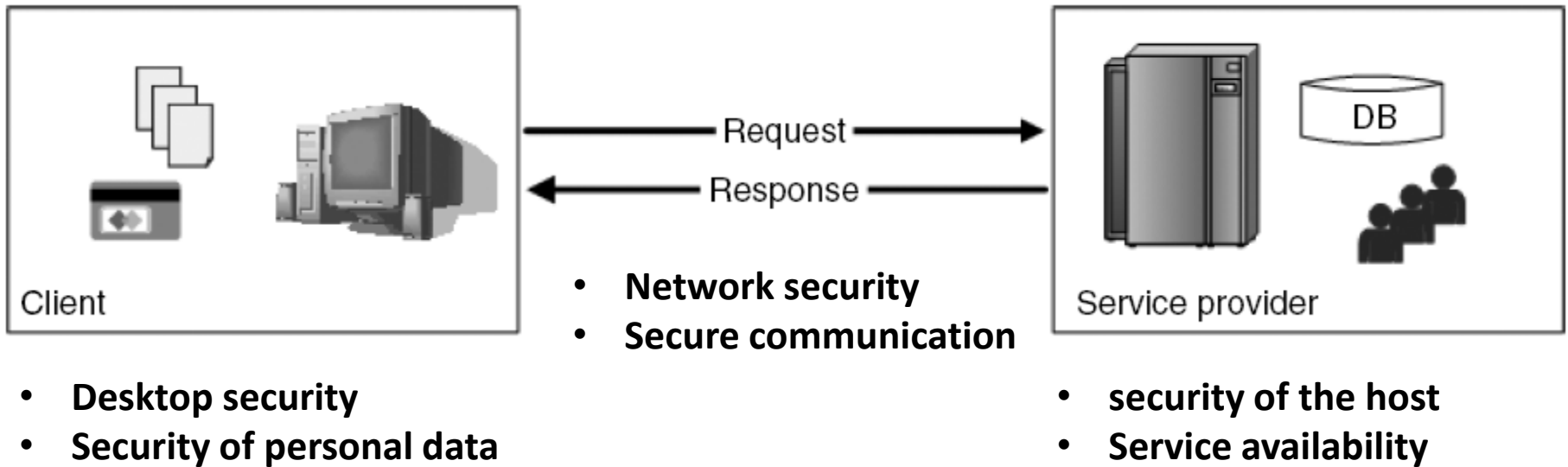
1. Web security...

- Several **risks** exist for service providers as well
 - **prevent** access from attackers
 - credit card number can be **stolen**
 - data can be **accessed and modified**
 - **availability** of service can be reduced
- can influence agreements and cause financial lose

1. Web security...

- **We can define security according to notions of users and service providers as**
 - securing the end **user's computer** and personal data stored on it
 - securing information in **transit**
 - securing the **server** and data stored on it

1. Web security...



1. Web security...

- **Security aspects**
- **Confidentiality:**
 - means communication between a customer and a provider **cannot** be read by a third party
 - **data encryption** can be used
- **Integrity:**
 - nobody is able to **modify** the exchanged information

1. Web security...

- **Security aspects**
- **Non-repudiation:**
 - originators of messages should not be able to **deny**
 - customers ordering books at an online store
- **Authentication:**
 - the process of verifying the **identity** of a person or general subject such **as another application** invoking a service on behalf of a human user
 - usually **implemented** by login/password mechanism

1. Web security...

- **Security aspects**
- **Authorization**
 - is used to **infer** which **privileges** authenticated users are granted
- **Availability**
 - guaranteeing the availability of Web applications
 - service downtime typically implies **financial losses**

1. Web security...

- **Security aspects**
- **Privacy**
 - privacy demands the **reliable handling** of data

2. Data encryption

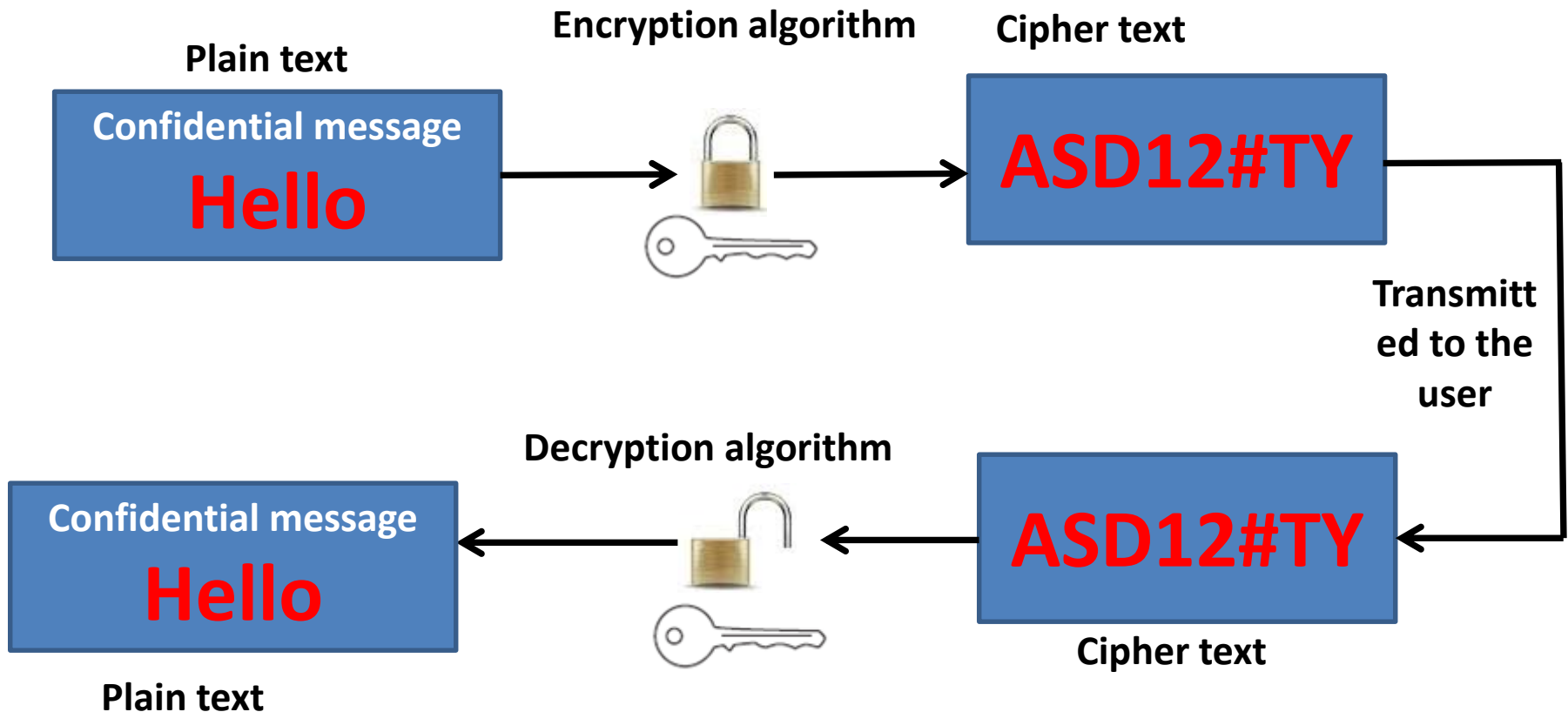
- Encryption is a basic technology for enabling **secure messaging**
- Encryption :
 - **translation** of data into a format that is intended to be unreadable by anyone except the intended party
 - **changing** the original text to a secret message using mathematical function
 - one-way encryption
 - two-way encryption

2. Data encryption...

- **Decryption:**
 - **changing** the secret message back to its original form

2. Data encryption...

- **Encryption/decryption process:**



2. Data encryption...

- Used by **Julius Caesar**
- Caesar shifted each letter of his messages to his generals **three places** down in the alphabet
- So **BURN THE BRIDGE** becomes
- **EXUQ WKH EUKFIG**

| | | |
|---|---|---|
| A | ⇒ | D |
| B | ⇒ | E |
| C | ⇒ | F |
| D | ⇒ | G |
| E | ⇒ | H |
| F | ⇒ | I |
| G | ⇒ | J |
| H | ⇒ | K |

2. Data encryption...

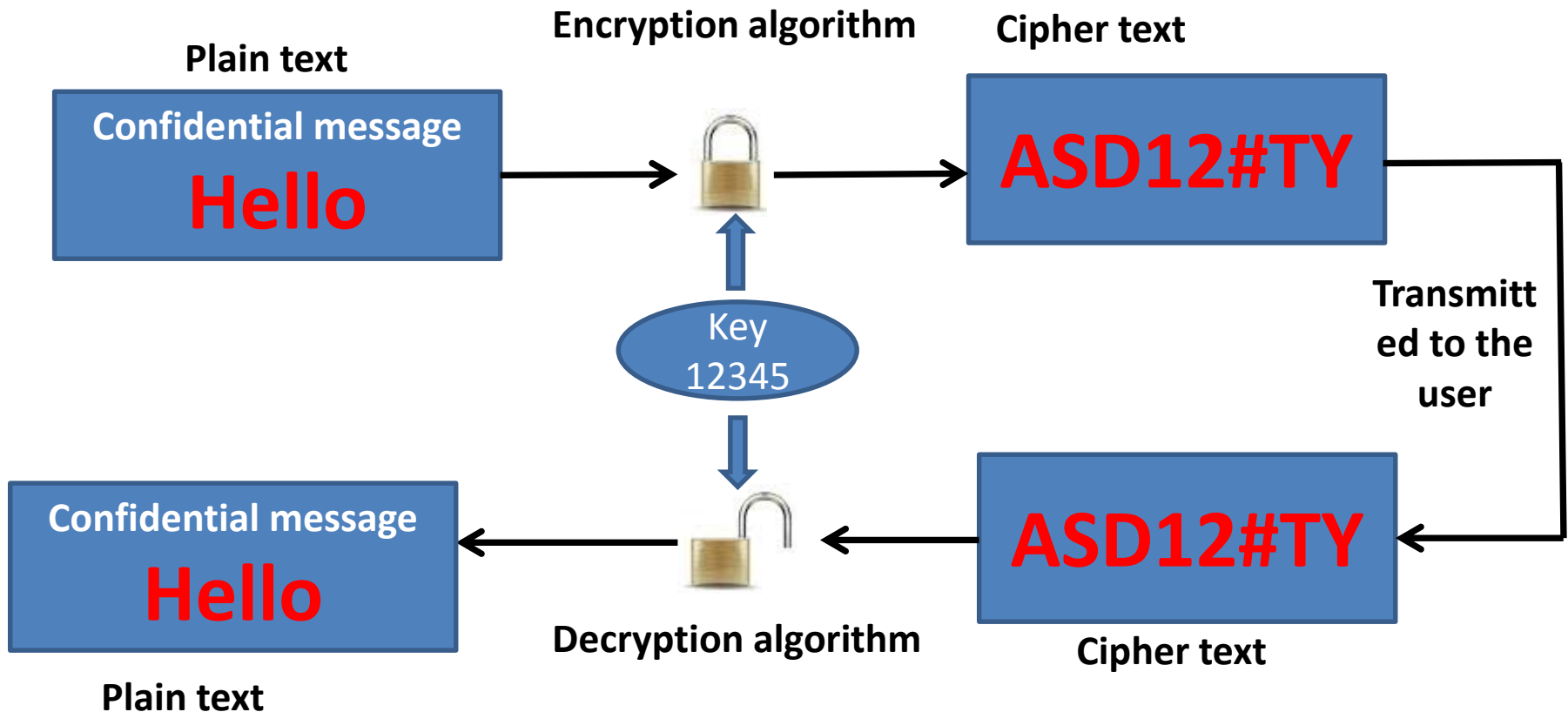
- **Cryptographic algorithms:**
- **Rely** on keys as secret term for **ciphering** and **deciphering**
- Without key it is **computationally** impossible to break an algorithm
- An algorithm is considered **strong** if brute force attack is the only **possible attack**

2. Data encryption...

- **Symmetric cryptography:**
- **Two-way encryption**
- **Use the **same single** key to encrypt and decrypt a message**
- **Also called **private key** cryptography**
 - **DES** and **AES** are examples of symmetric cryptographic algorithms

2. Data encryption...

- **Symmetric cryptography:**

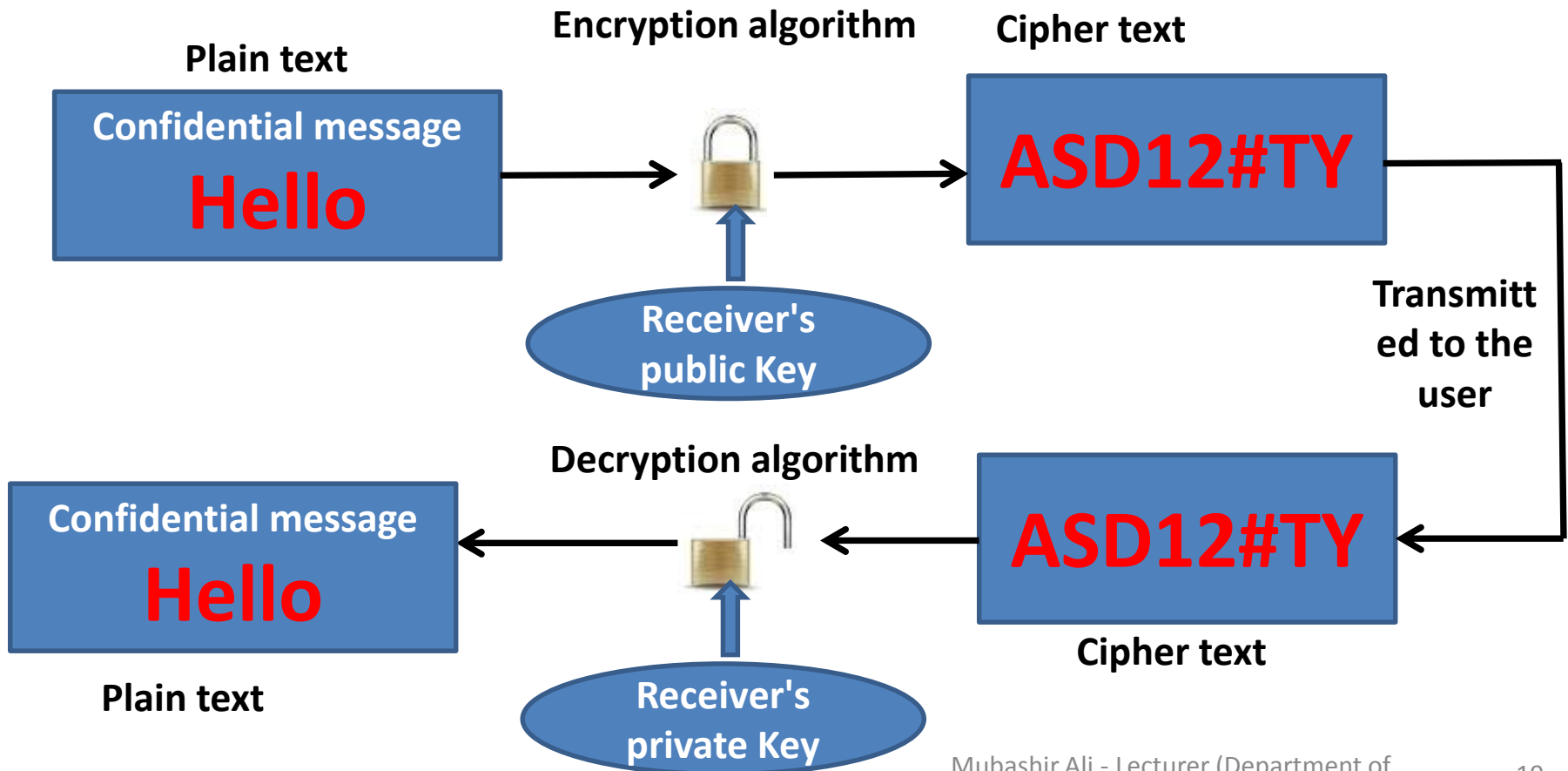


2. Data encryption...

- **Asymmetric cryptography:**
- Also known as **public key** cryptography
- Uses **two keys** instead of one
 - The **public key** is known to everyone and can be freely distributed
 - The **private key** is known only to the recipient of the message
- **RSA is an example of asymmetric cryptography**

2. Data encryption...

- **Asymmetric cryptography:**



2. Data encryption...

- **Hashing algorithms:**
- **Hashing is a **one-way process****
 - converting a hash back to the original data is difficult or impossible
- **A hash is a unique “signature” for a set of data**
 - this signature, called a hash or digest, represents the contents

2. Data encryption...

- **Digital signatures:**
- **A digital signature is basically a way to **ensure** that an electronic document is **authentic****
 - Integrity
 - Non repudiation

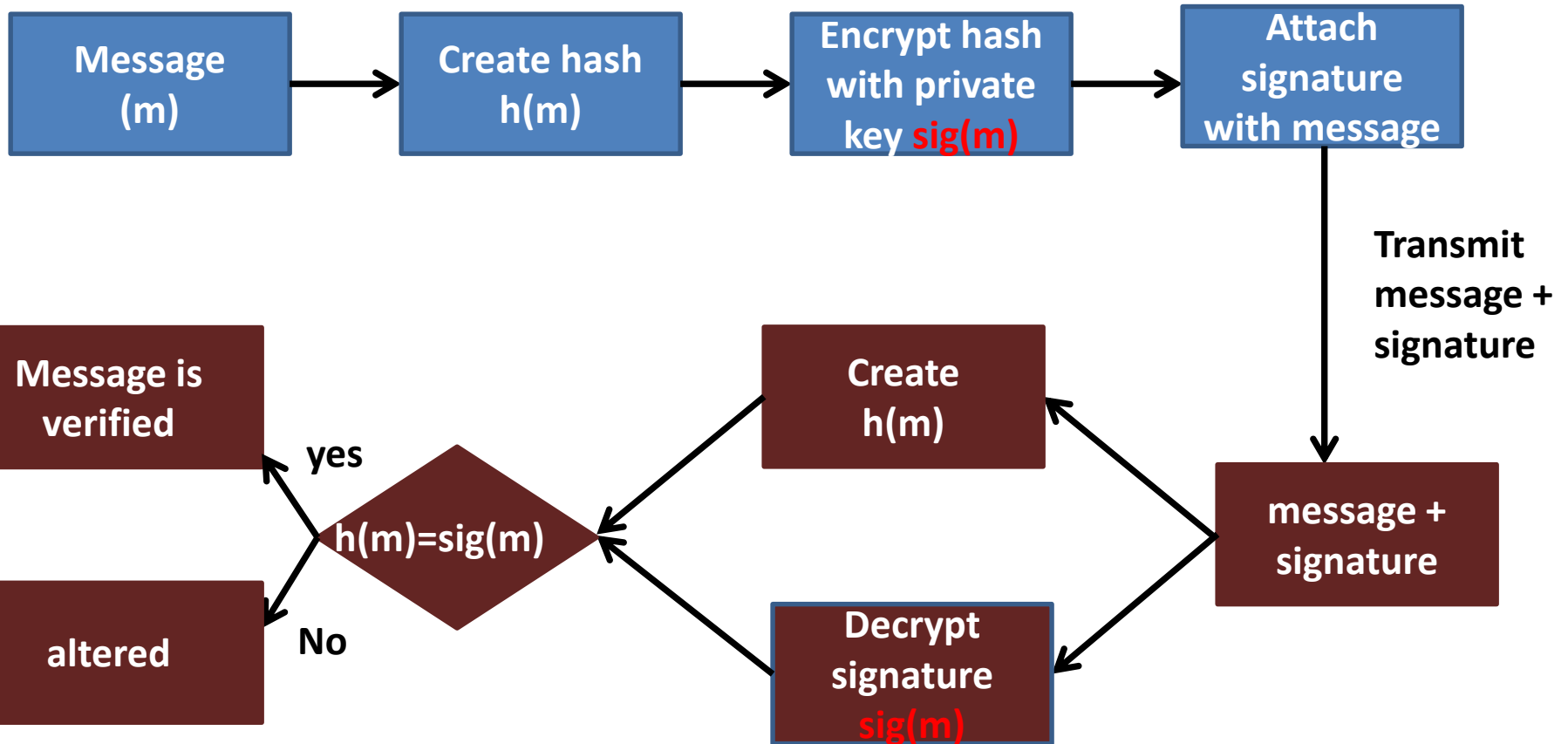
2. Data encryption...

- **Digital signatures creation:**
- **sender creates a hash of the message**
- **sender encrypts the message with his/her private key**
- **attach the digital signature with message**

2. Data encryption...

- **Digital signatures validation:**
- **Receiver decrypts the signature with sender's public key**
- **Receiver creates the hash of the message**
- **Created hash is compared with the decrypted message**

2. Data encryption...



3. Data encryption....

- **Cryptography ensures**
 - **Confidentiality**
 - **Integrity**
 - **Availability**
 - **Authenticity**
 - **Non-repudiation**

3. Securing user's data

- **After securely transmitting data user wants**
- **Privacy**
 - providers keep data **carefully**
 - **protect** data from attackers
- **Secured desktop**

3. Securing user's data...

- **Service providers need to establish trust relationship**
 - can **specify** data practices using platform for Privacy Preferences (P3P) standard
- **User can specify its preferences using P3P-agent**
- **P3P-capable browsers inform the user if service provider's policies conflict with user's preferences**

3. Securing user's data...

- **Phishing and Web Spoofing**
- **Phishing** is the most common attack to retrieve user's personal information
- **Web spoofing** denotes **mocking** the web presence of famous companies
 - **send email** to users as representative of some well known company
 - **encourage** the user's to enter their personal information

3. Securing user's data...

- **Securing the desktop**
- **users' security can be at-risk through threats like viruses and worms**
 - it is user's **responsibility** to tackle with them

3. Securing user's data...

- **Adware and spyware**
 - adware deliver **advertising contents**
 - spyware **monitor** users activities and **transfer** gathered information to remote systems
- **Remote access/backdoors**
- **provide remote systems the ability to connect with user's machine**
 - can **obtain** personal information, damage files and control user's machine

3. Securing user's data...

- **Viruses**
- can **damage** files or **repeat** themselves
 - distributed through email or by sharing infected files
- **Worms**
- **Repeat themselves**
 - **increase** traffic and **consume** processing power

3. Securing user's data...

- Trojan horses
- Damage files but don't replicate
- Appears as useful programs but performs other functionalities
 - aims at **data theft** and **destruction** or **illegitimate access** on computational resources

4. Service providers issues

- Service provider wants to **secure** the server from **attackers**
- Common attacks:
- Cross-site scripting (XSS)
- Attackers **inject script** in dynamically created pages and try to find user's information
- SQL-injection
- Attackers **inject sql** commands as an input

Summary

- **Web security overview**
- **Secure transmission of data**
- **User's security issues**
- **Service provider's issues**

References

- **Chapter 13**, Kappel, G., Proll, B. Reich, S. & Retschitzegger, W. (2006). **Web Engineering**, Hoboken, NJ: Wiley & Son