# CO 487: Applied Cryptography

Chapter 0: Course Preview

October 24, 2019

# 1 Introduction to Cryptography

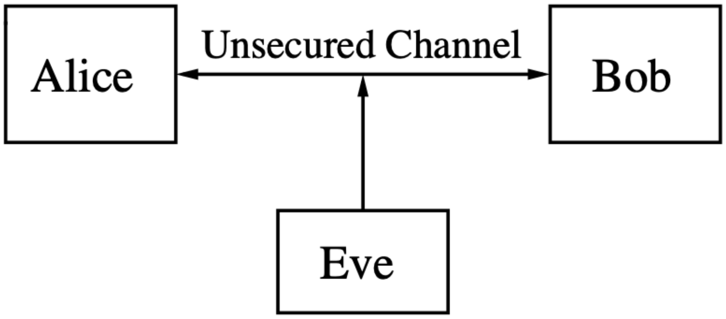
**Definition**: **Cryptography** is a subject of securing communications from malicious adversaries such as reading, modifying, injecting and deleting data without authorizations.

1. **Confidentiality**: Keeping data secret from all but those authorized to see it.

2. **Data Integrity**: Ensuring data has not been altered by unauthorized means.

3. **Data Origin Authentication**: Corroborating the source of data.

4. **Non-Repudiation**: Preventing an entity from denying previous commitments or actions.



## 2 Secure Web Transactions (SSL)/Transport Layer Security(TLS)

**Definition**: **Secure Web Transactions (SSL)/Transport Layer Security(TLS)** is the cryptographic protocol used by web browsers for

- securing web transactions
- assuring the users of browsing the authenticity of the website
- establishing a secure communications channel.

**Example**: Credit card payments, secure access to social network sites.

**Definition**: **Clients** are individual users.

**Definition**: **Servers** are web sites.

**Definition**: **Keys** are the secret information $k$ shared by the client and the server.

**Definition**: **Symmetric-key Cryptography** means that the client and server a priori share some secret information, which is a key. Symmetric-key cryptography can subsequently engage in secure communications by encrypting their messages with AES and authenticating the resulting ciphertexts with HMAC.

**Definition**: **Public-key Cryptography** means that communicating parties a priori share some authenticated (but non-secret) information.

1. The client selects the secret session key $k$.
2. Encrypts it with the server's RSA public key.
3. The servers, the only one can decrypt, decrypt the resulting ciphertext with its RSA private key.

**Definition**: **Signature Scheme** is the server's RSA public key is signed by a Certifying Authority using the RSA signature scheme. The client can verify the signature using the Certifiying Authority's RSA public verification key which is embedded in its browser, so that the clients obtains an authentic copy of the server's RSA public key.

## 3 The TLS Protocol and its Vulnerabilities

How the **TLS Protocol** works:

1. The server transmits its certificate to the client when the client visits a secured web page.
   - The certificate contains the server's identifying information (e.g., web site name and URL) and RSA public key, and the RSA signature of a certifying authority.
   - The certifying authority is trusted to carefully verify the server's identity before issuing the certificate.
2. The client verifies the signature using the certifying authority's public key upon the receipt of the certificate.
   - A successful verification confirms the authenticity of the server and of its RSA public key.
3. The client selects a random session key $k$, encrypts it with the server's RSA public key, and transmits the resulting ciphertext to the server.
4. The server decrypts the ciphertext to obtain the session key, which is then used with symmetric-key schemes to encrypt and authenticate all sensitive data exchanged for the remainder of the session.
5. The establishment of a secure link is indicated by a closed padlock in the browser.

The **Potential Vulnerabilities** of TLS:

- The crypto is weak.
- Quantum attacks on the underlying cryptography.
- Weak random number generation.
- Issuance of fraudulent certificates.
  - Mistake due to human error.
- Software bugs.
- Phishing attacks.
  - Most users do not verify the security information by looking at the URL.
- TLS only protects during transit. It does not protect the data when it is collected at the server.

  - Many servers store credit card data and other personal information.

- The National Security Agency.

**Cryptography is not equal to security.**

Cryptography provides some mathematical tools that can assist with the provision of cybersecurity services. It is a small but essential part of a complete security solution. Security is a chain. Weak links become targets; one flaw is all it takes. Cryptography is usually not the weakest link. However, when the crypto fails the damage can be catastrophic.

**Cryptography is multi-disciplinary.**

- Math: Design and analysis of problems that are believed to be hard.
- Computer science: Design and analysis of cryptographic protocols whose security relies on the hardness of the underlying math problem.
- Engineering: Efficient and secure implementation of the protocols in hardware and software.