Cryptography is everywhere

Secure communication:

- web traffic: HTTPS
- wireless traffic: 802.11i WPA2, GSM, Bluetooth

Encrypting files on disk: EFS, TrueCrypt

Content protection (e.g. DVD, Blu-ray): CSS, AACS

User authentication

- Cryptography is not the ultimate solution for the security. It is the basic building block for security approach.
- Even though encryption algorithm is safe we face many other problems and challenges.
- **User Authentication:** User Authentication is to prove to the system that who you are. Username and Password are the procedure to prove who you are.

There are two parts in TLS.

Secure Sockets Layer / TLS

Two main parts

1. Handshake Protocol: **Establish shared secret key using public-key cryptography** (2nd part of course)

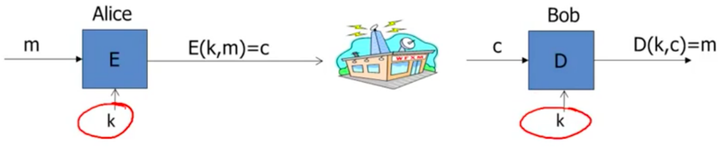
2. Record Layer: **Transmit data using shared secret key**
   Ensure confidentiality and integrity (1st part of course)

- There are two types of encryption algorithm.

1. One is called public cryptography sometimes called as asymmetric encryption algorithm, which means they are not similar. There is one called public key and another private key. When encrypting we use different key and while decrypting we use another key. - RSA
2. Symmetric encryption algorithm - This approach is extensively follow in the video where the encryption key and decryption key are the same. This is called symmetric because the two keys are the same. But, some time there might be different encryption/decryption keys. However, we can derive out the one key by the another key so still it is Symmetric Encryption.

Is a Asymmetric algorithm is always more secure then symmetric algorithm?
No.

Building block: sym. encryption



E, D: cipher k: secret key (e.g. 128 bits)
m, c: plaintext, ciphertext

Encryption algorithm is publicly known

- Never use a proprietary cipher

Use Cases

Single use key: (one time key)

- Key is only used to encrypt one message
  - encrypted email: new key generated for every email

Multi use key: (many time key)

- Key used to encrypt multiple messages
  - encrypted files: same key used to encrypt many files
- Need more machinery than for one-time key

Things to remember

Cryptography is:

- A tremendous tool
- The basis for many security mechanisms

Cryptography is not:

- The solution to all security problems
  - Software bugs
  - Social eng. attacks
- Reliable unless implemented and used properly
- Something you should try to invent yourself
  - many many examples of broken ad-hoc designs