COMPUTER SECURITY

Securing communications

Lecture 4

4th stage – (2021-2022)

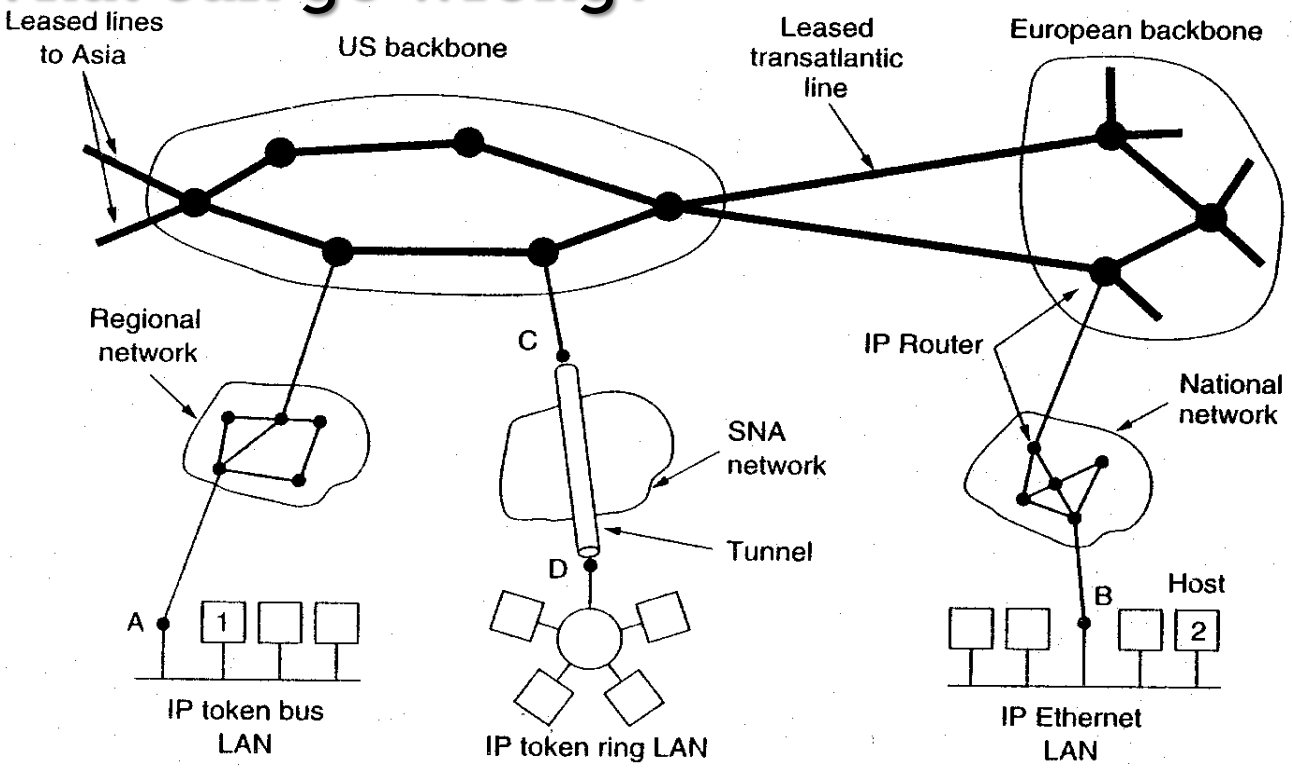
Dr. Moceheb Lazam Shuwandy

COMPUTER SECURITY AND COMMUNICATIONS

- **Securing communications**
  - **Three steps:**
    - **Secrecy = prevent understanding of intercepted communication**
    - **Authentication = establish identity of sender**
    - **Integrity = establish that communication has not been changed**

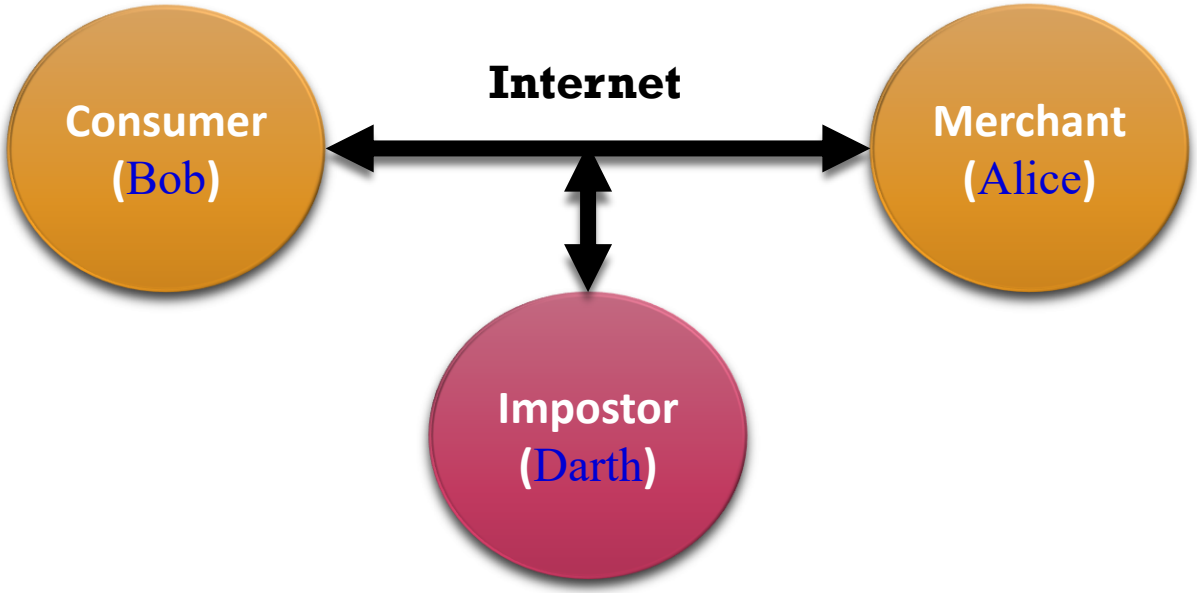
SECURING COMMUNICATIONS

- What can go wrong?

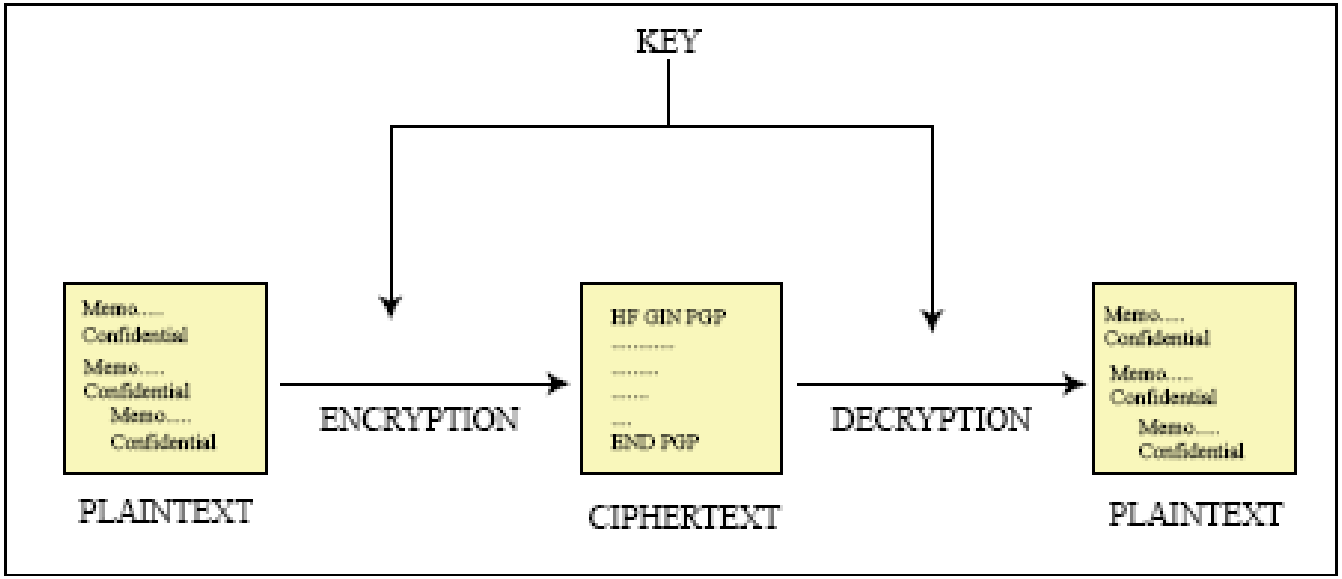


COMMUNICATIONS SECURITY ISSUES

- Encryption - How do I ensure the secrecy of my transactions?
- Authentication - How do I verify the true identity of my counterparts?
- Integrity - How can I be sure the message hasn't been altered?

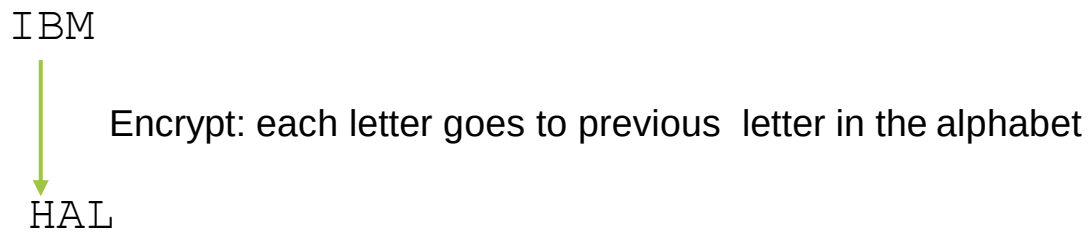


ENCRYPTION- TRADITIONAL CRYPTOGRAPHY



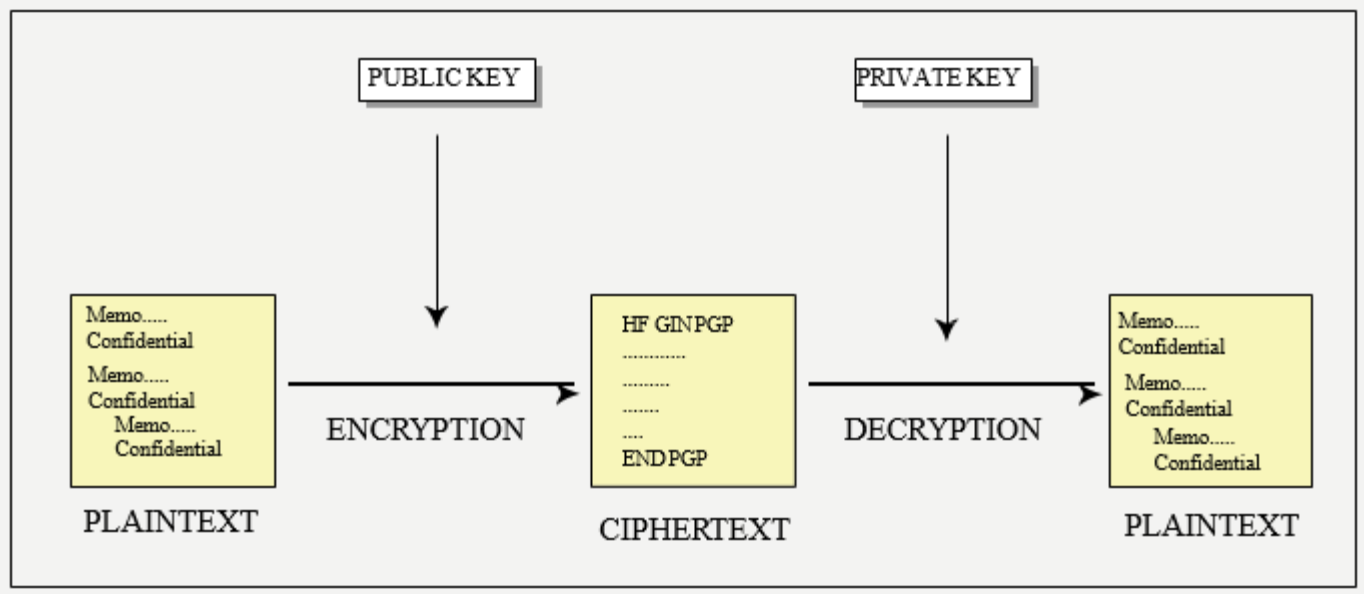
CEASAR'S CIPHER: ENCRYPTION BY SUBSTITUTION

- **Substitute for each letter (block of bits)**



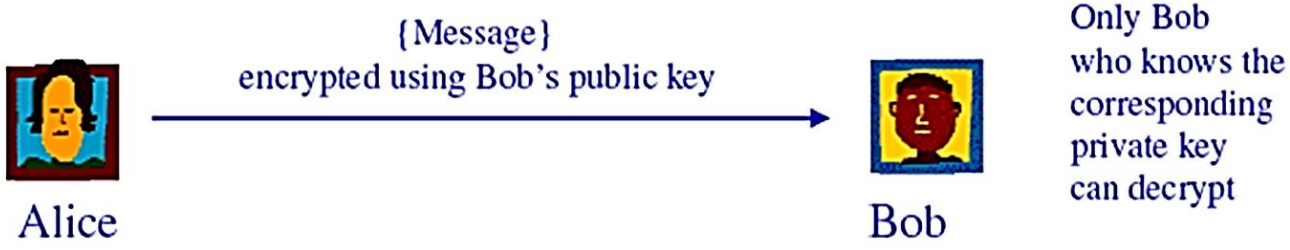
- **How can you crack a substitution cipher?**
  - **I.e., how can you guess the key?**

PUBLIC-KEY CRYPTOGRAPHY



PUBLIC KEY CRYPTOGRAPHY..CON.

- Secret key cryptography: Based on a secret key
  - Same secret key used for encryption and decryption
  - Problem: How to transmit key securely on the Internet???
- Public key cryptography: Two keys used
  - Public key known to everybody. Used for encryption.
  - Private key known only to owner. Used for decryption.



PUBLIC KEY CRYPTOGRAPHY WORKS IF…

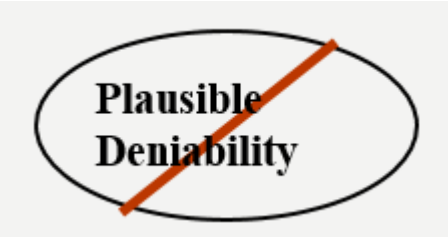
- Private key remains secret
  - Never leaves the owner's computer
  - Typically encrypted and password-protected
- Difficult to guess private key from knowledge of public key
  - Boils down to trying all different key combinations
  - Difficulty of "breaking" the code rises exponentially with the bit length of the key
  - 1024-bit keys require more time than the life of the universe in order to be "broken"
- Reliable public key distributed
  - This is the most difficult problem!

ENCRYPTION IS NOT ENOUGH: SPOOFS

- Pretending to be someone else
- Hard to login without someone's password
- But can send out communications with someone else's name on it
  - email
    - 1993: Dartmouth sent a message saying midterm exam was cancelled
    - Message appeared to come from the Professor!

NEEDED: MESSAGE AUTHENTICATION

- Make sure Bob gets the message unaltered
- Don't let Alice deny sending the message



- Don't care about eavesdropper Darth, unless Darth changes the message
- How can cryptography help?

DIGITAL SIGNATURES

- **Key property**: Public and private keys can be applied in either order

- **Alice has message M**
  - She applies her private key to it
  - She sends encrypted message to Bob

- **Bob decrypts it with Alice's public key**
  - gets back original message
  - infers that Alice is indeed the sender (since only Alice has the private key that corresponds to her public key)

- In that way, encrypting a message with one's private key acts as a digital signature!

PUBLIC KEY MANAGEMENT

- Public key cryptography works as long as
  - Private key is really kept secret
  - Hard to compute private key from public key
  - Get the correct public key from some trusted source
- Bob can send public key over insecure communication channel
- But how do you know Darth didn't send you his key instead?

A CENTRAL KEY DISTRIBUTOR

- Alice asks the distributor for Bob's public key
- The distributor sends it to Alice and "digitally signs" it
- Alice knows the key came from the distributor
  - ✓ Now just have to be sure that the distributor is honest and got Bob's key from Bob, not Darth
- Requires one secure communication per user
  - ✓ Bob sends public key to distributor when he joins the system
- Secret keys require secure communication between every pair of users

PUBLIC KEY INFRASTRUCTURE (PKI)

- Certificate Authorities are Trusted Third Parties charged with the responsibility to generate trusted certificates for requesting individuals organizations
  - Certificates contain the requestors public key and are digitally signed by the CA
  - Before a certificate is issued, CA must verify the identity of the requestor

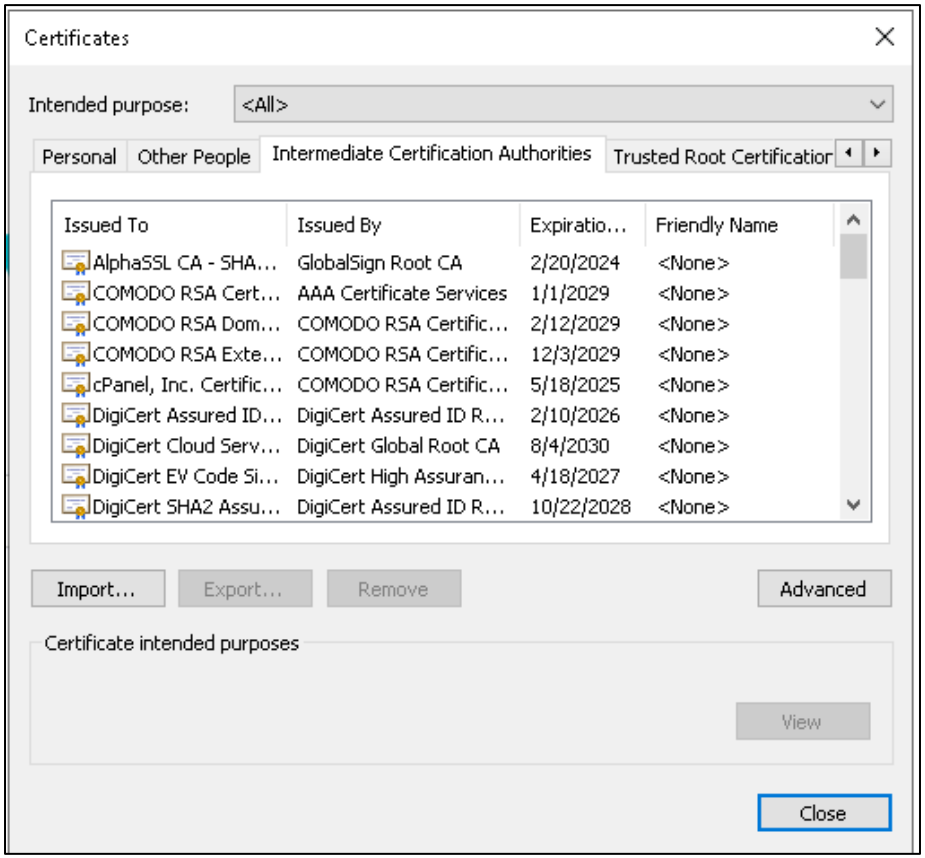
- These certificates can then facilitate automatic authentication of two parties without the need for out-of-band communication

CERTIFICATES

- Used to certify a user's identity to another user
  - The certificate issuer's name
  - Who the certificate is being issued for (a.k.a the subject)
  - The public key of the subject
  - Some time stamps
- Digitally signed by issuer
- Issuer must be a trusted entity
- All users must have a reliable public key of the issuer
  - in order to verify signed certificate

WEB BROWSERS

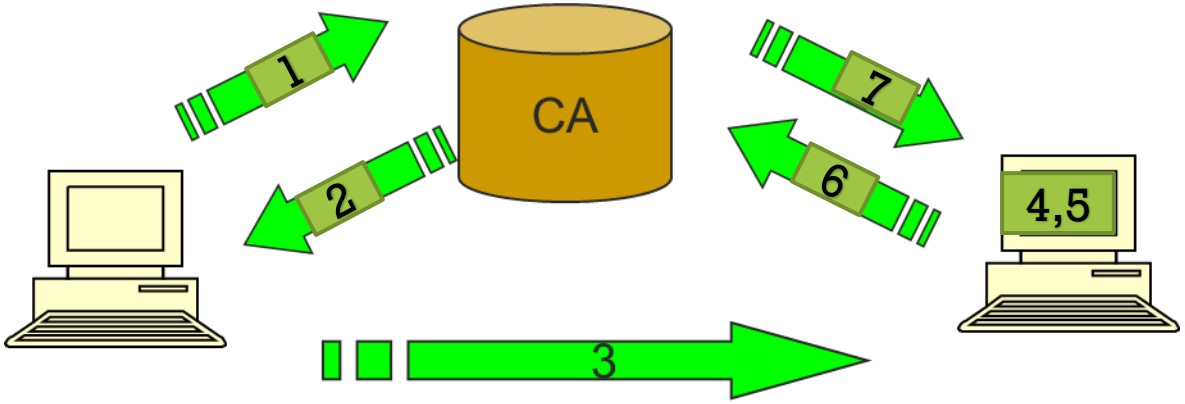
- They come with a number of certificates already installed



PKI INDUSTRY

- Main players: trusted third party CAs
  - Verisign
  - Entrust
  - Cybertrust
  - RSA
- Revenue from
  - products (PKI servers for intranets and extranets)
  - services (certificate services for individuals and organizations)

SUMMARY – PERSONAL COMMUNICATIONS



A wants to send an encrypted message to **B**, including digital signature of **A**

1)A recalls public key of **B** from **CA**

2)CA sends public key of **B to A**

3)A applies its private key to the message and sends it encrypted by public key of **B**

4)Reception by B

5)B decrypts message with its own private key

6)B recalls **A's** public key from **CA**

7)CA sends public key of **A to B,** assuring the message was sent by **A**

APPLICATIONS: ECOMMERCE SECURITY

- Needed to transmit sensitive information through the Web
  - credit card numbers
  - merchandise orders
- Requirements
  - sender and receiver must authenticate each other before sending any "real" data
  - all "real" data must flow encrypted through the network
  - no intercepted communication can be used to an intruder's advantage

SSL / TLS

- Secure Sockets Layer / Transport Layer Security
- Provides reasonable level of security
- Often used for transactions between consumers and merchants

SSL / TLS…CON.

Negotiate Security Options

Merchant's digital certificate

Customer

Merchant

Random session key generated by customer
and encrypted with merchant's public key

Ongoing communication with
both parties using session key

APPLICATIONS: VIRTUAL PRIVATE NETWORKS (VPN)

- Secure, private networks that operate over a public network (like the Internet).
  - Messages are confidential
  - Only authorized users can access network
- "Tunneling" --encrypted messages from one protocol are packaged inside another protocol.

Q&A