Information Security
CS 3002

Dr. Haroon Mahmood

Assistant Professor

NUCES Lahore

Design of Security Architecture

- **Defenses in Depth,**
  - **Implementation of security in layers, policy, training, technology.**
  - **Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls**

- **Security Perimeter**
  - **Point at which an organization's security protection ends and outside world begins**
  - **Does not apply to internal attacks from employee threats or on-site physical threats**

Key Technology Components

- **Firewall**
  - Device that selectively discriminates against information flowing in and out
  - Specially configured computer
  - Usually on parameter part of or just behind gateway router

- **Proxy Server**
  - Performs actions on behalf of another system
  - Configured to look like a web server
  - Assigned the domain name
  - Retrieves and transmits data
  - Cache server

Key Technology Components

- DMZ
  - Buffer against outside attacks
  - No mans land between computer and world
  - Web servers often go here
- IDS
  - Intrusion Detection System
    - Host based
      - Installed on machines they protect
      - Monitor host machines
    - Network based
      - Look at patterns of network traffic
      - Attempt to detect unusual activity
      - Requires database of previous activity
      - Uses “machine learning” techniques
      - Can use information form similar networks

Security Architecture

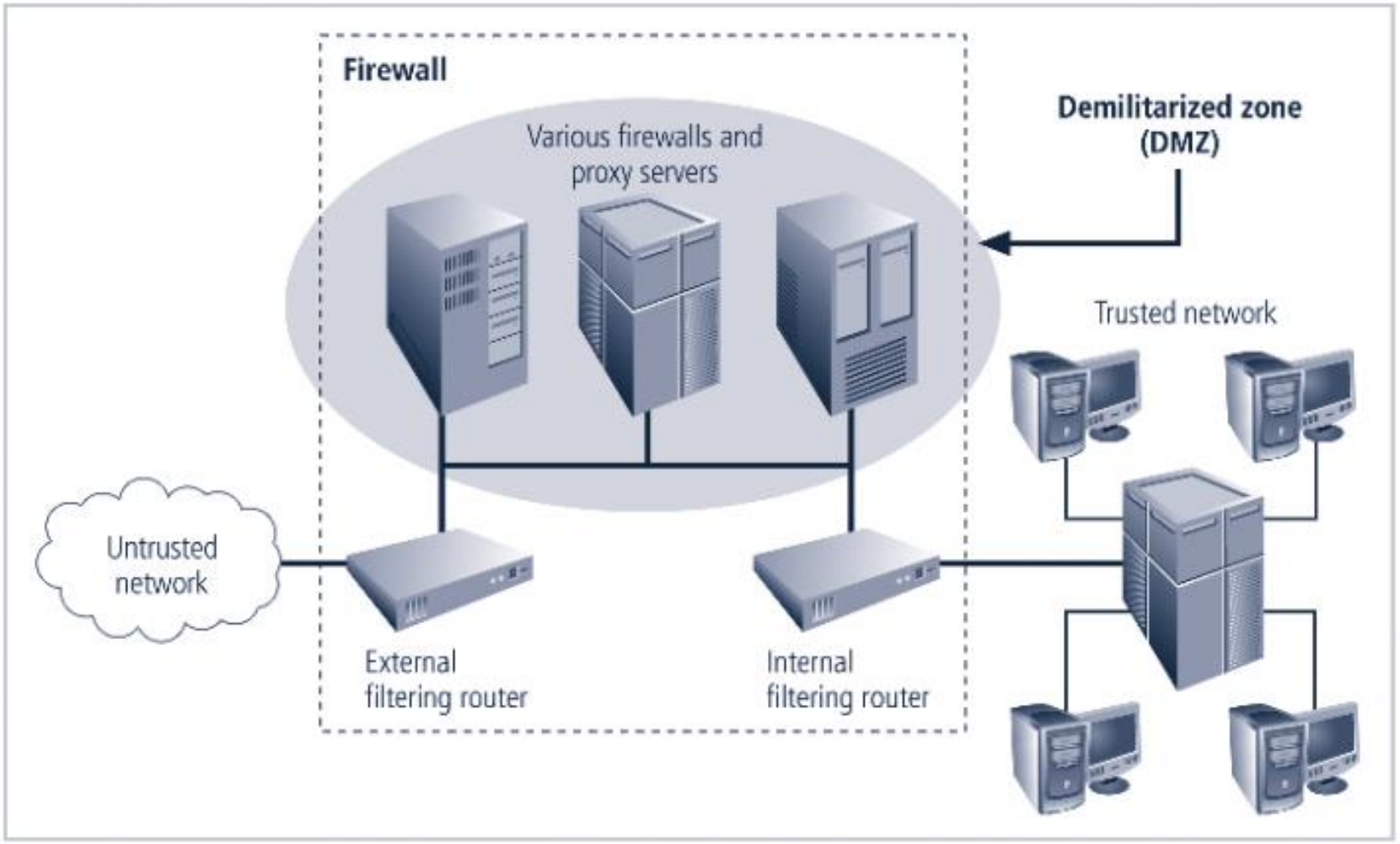


FIGURE 5-18 Firewalls, Proxy Servers, and DMZs

Secure Communication and Storage

- **Vulnerable components**
  - Channels
  - Processes (clients, servers)

- **Security properties:**
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Availability

Types of cryptographic functions

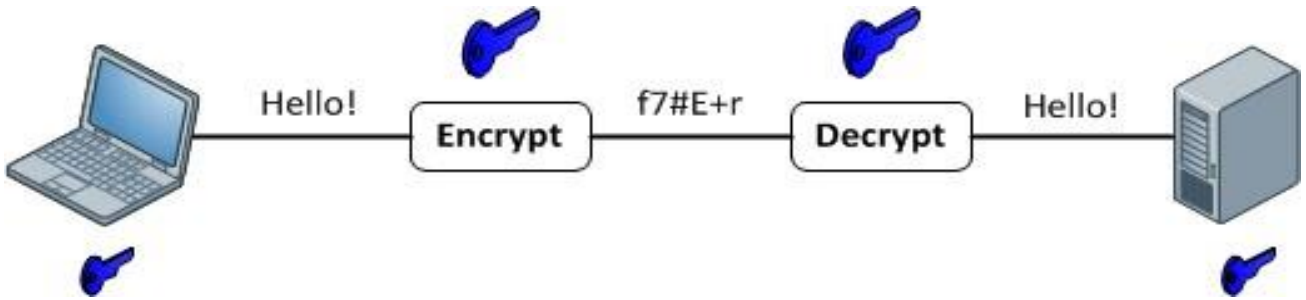
- **Secret/symmetric key cryptographic function**
  - **Uses 1 key**
  - **Fast computation**
- **Public/Asymmetric key cryptographic function**
  - **Uses 2 keys**
  - **Slow computation**
- **Hash functions**
  - **Uses no keys**
  - **Very fast computation**

Key terms

- **Plaintext**
  - **Readable message or data that needs to be protected**
- **Encryption Algorithm**
  - **Algorithm to perform various substitutions and transformations on the plaintext**
- **Secret key**
  - **Used as input to the algorithm, transformations depend on the key**
- **Ciphertext**
  - **Scrambled message produced as output**
- **Decryption Algorithm**
  - **Produces the original plaintext**

Symmetric/secret key encryption

- Also called conventional cryptography
- Sender and receiver must both know the secret key
- Uses techniques like confusion and diffusion to encrypt/decrypt data



Symmetric encryption uses

- Transmitting over secure channel
- Secure storage on insecure media

- Authentication
  - Strong authentication: prove the knowledge of a secret without revealing it

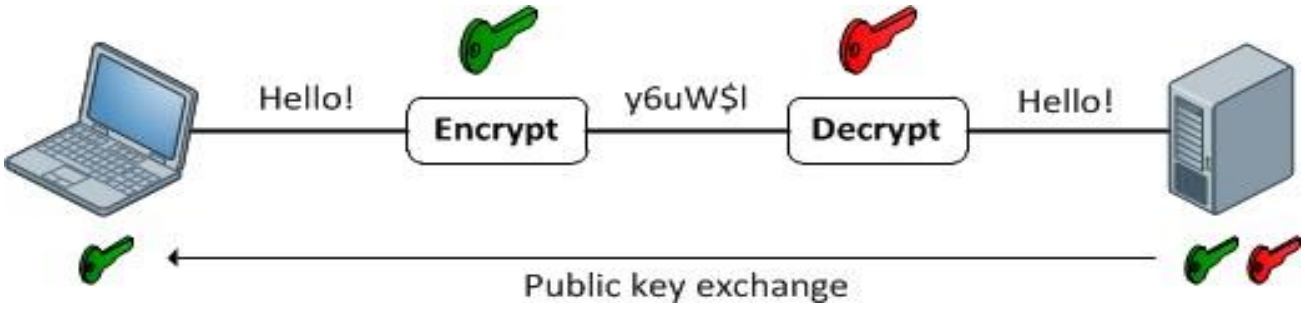
- Integrity check
  - Checksum vs cryptographic checksum
  - Message Authentication Code (MAC)/MIC

Problems with symmetric cryptography

- **No mechanism of sharing the key**
- **Impersonation problem**
  - **If Alice and bob share a key. Imagine Trudy shares the same key with Alice for secure communication. Trudy may act as alice and talk to bob.**
- **Difficult key management**

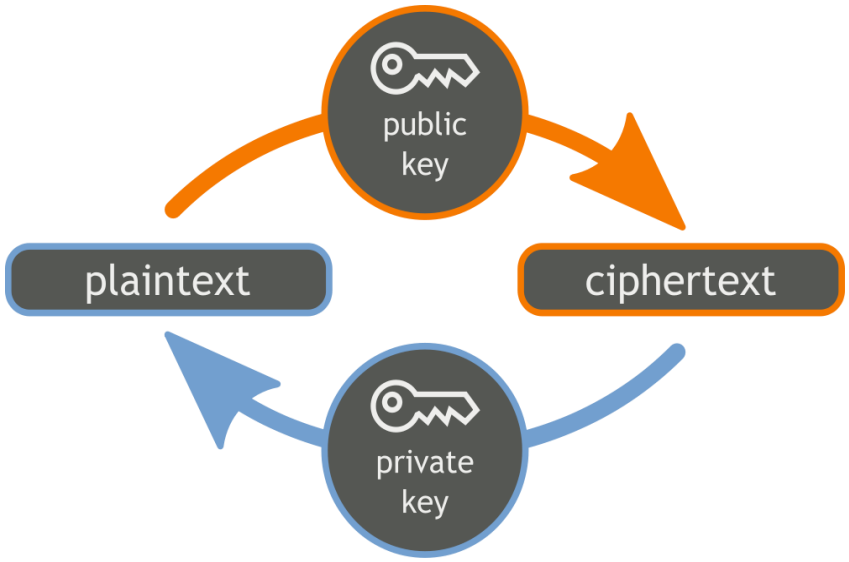
PUBLIC KEY CRYPTOGRAPHY

- Also called Asymmetric cryptography
- Rather newer form of cryptography – invented in 1975.
- Two keys – Public Key & Private Key
- Based on hard mathematical problems



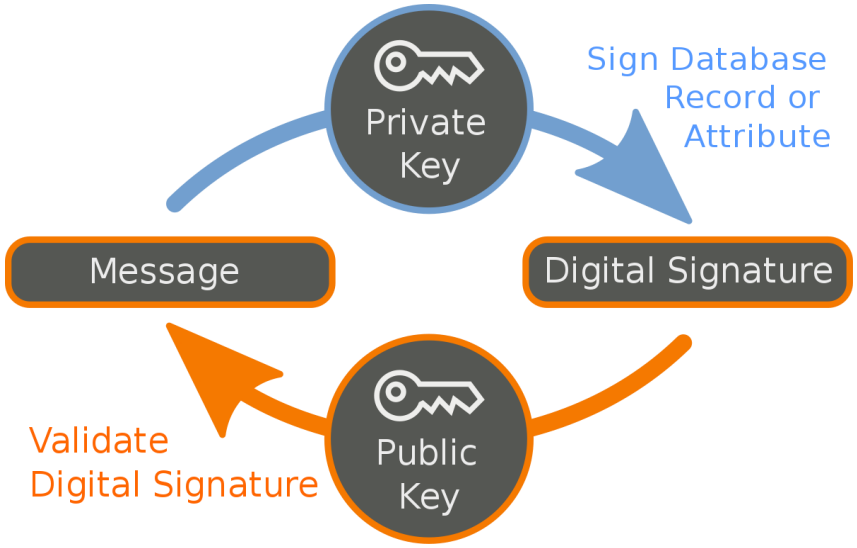
Public key encryption

- **The private key can unlock (decrypt) what is locked (encrypted) with the public key and vice versa**



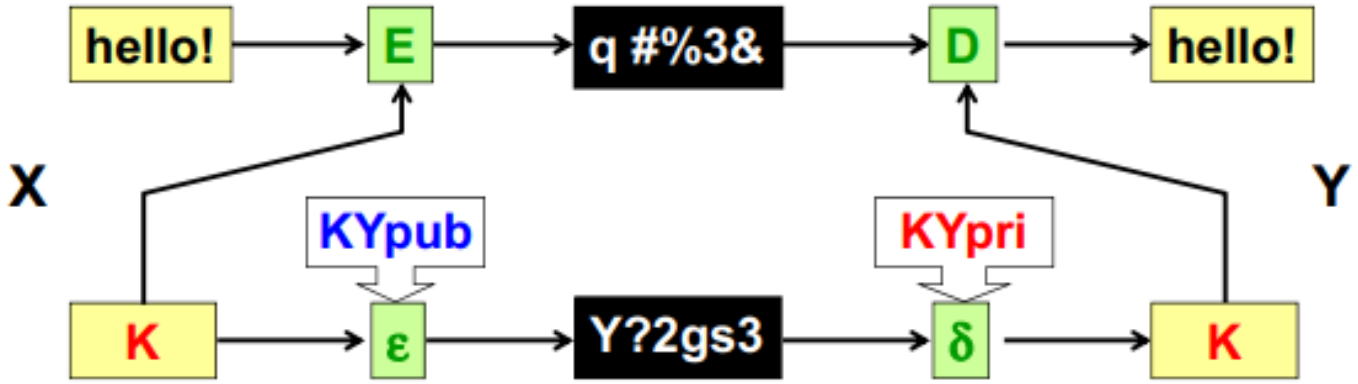
Digital signature

- **Scheme for proving the authenticity and origin of a message.**
- **Recipient is sure of the origin of the message**
- **Sender can not deny having sent**
- **the message(non-repudiation)**



Using PKC to share secret key

- **The key(K – which is the secret key NOT the private key) is encrypted using the Public key of Y so that the key(K) is shared between X and Y only. Then that K is used for encryption of data(hello!)**



Public Key Cryptography Uses

- Used primarily for Symmetric key exchange
- Transmitting over an insecure channel
- Secure storage on insecure media
- Authentication
- Easy key management
- Digital signatures
  - Non-repudiation
  - Data integrity

Symmetric Encryption

E, D: Algorithms **k: secret key**

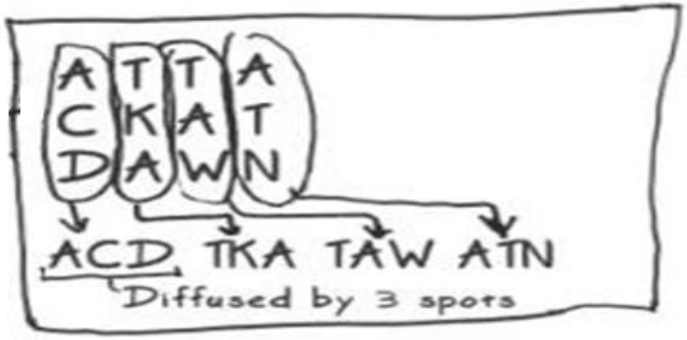
m: plaintext **c: ciphertext**

Encryption algorithm Should be publicly known

Early days techniques

- **Confusion**
  - **Replacing of some bit strings with other bit strings**
  - **Also called substitution or Caesar's cipher**

- **Diffusion**
  - **Changing order of bit strings**
  - **Also called permutation/transposition**



Question

What is the size of key space in the substitution cipher assuming 26 letters?

$$|\mathcal{K}| = 26$$

$$|\mathcal{K}| = 26!$$

$$|\mathcal{K}| = 2^{26}$$

$$|\mathcal{K}| = 26^2$$

Breaking of Substitution Cipher

(1) Use frequency of English letters

E, I,T, A

(1) Use frequency of pairs of letters (di-grams)

an , in , the

Example

UKBYBIPOUZBCUFEEBORUKBYBHOBBRFESPVKBWFOFERVNBCVBZPRUBOFERVNBCVBPCYY
FVUFOFEIKNWFRFIKJNUPWRFIPOUNVNIPUBRNCUKBEFWWFDNCHXCYBOHOPYXPUBNCU
BOYNRVNIWNCPOJIOFHOPZRVFZIXUBORJRUBZRBCHNCBBONCHRJZSFWNVRJRUBZRPCYZ
PUKBZPUNVPWPCYVFZIXUPUNFCPWRVNBCVBRPYYNUNFCPWWJUKBYBIPOUZBCUIPOUN
VNIPUBRNCHOPYXPUBNCUBOYNRVNIWNCPOJIOFHOPZRNCRVNBCUNENVVFZIXUNCHPCY
VFZIXUPUNFCPWZPUKBZPUNVR

B	36
N	34
U	33
P	32
C	26

➔ E

➔ I

➔ T

➔ A

NC	11
PU	10
UB	10
UN	9

Di-grams

➔ IN

➔ AT

UKB	6
RVN	6
FZI	4

Tri-grams

➔ THE

Vigenere Cipher

- **Idea: Uses Caesar's cipher with various different shifts, in order to hide the distribution of the letters.**
- **A key defines the shift used in each letter in the text**
- **A key word is repeated as many times as required to become the same length**

Plain text:	I a t t a c k
Key:	2 3 4 2 3 4 2
Cipher text:	K d x v d g m

(key is “234”)

Breaking of Vigenere Cipher

- **Find repeated strings in the ciphertext. Their distance is expected to be a multiple of the length. Compute the gcd of (most) distances.**
- **For example:**
  - **Plaintext: TOBENOTORTOBE**
  - **Keyword: 1231231231231**
  - **Ciphertext: UQEFPRUQUUQEF**

Diagraph	First Position	Second Position	Distance	Factors
UQ	1	7	6	3
UQ	7	10	3	3
EF	3	12	9	3
QE	2	11	9	3