Encryption
Public Key

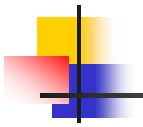
Dr.Talal Alkharobi

Public key (asymmetric) cryptography

2

- A form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key.
- The private key is kept secret, while the public key may be widely distributed.
- The keys are related mathematically, but the private key cannot be practically derived from the public key.
- A message encrypted with the public key can be decrypted only with the corresponding private key.

3



A postal analogy

- Alice has the secret message and wants to send it to Bob, after which Bob sends a secret reply through the public mail.
- With a symmetric key system,
  - Alice first puts the secret message in a box, and then locks the box using a padlock to which she has a key.
  - She then sends the box to Bob through regular mail.
  - When Bob receives the box, he uses an identical copy of Alice's key (which he has obtained previously, maybe by a face-to-face meeting) to open the box, and reads the message.
  - Bob can then use the same padlock to send his secret reply.

4

A postal analogy

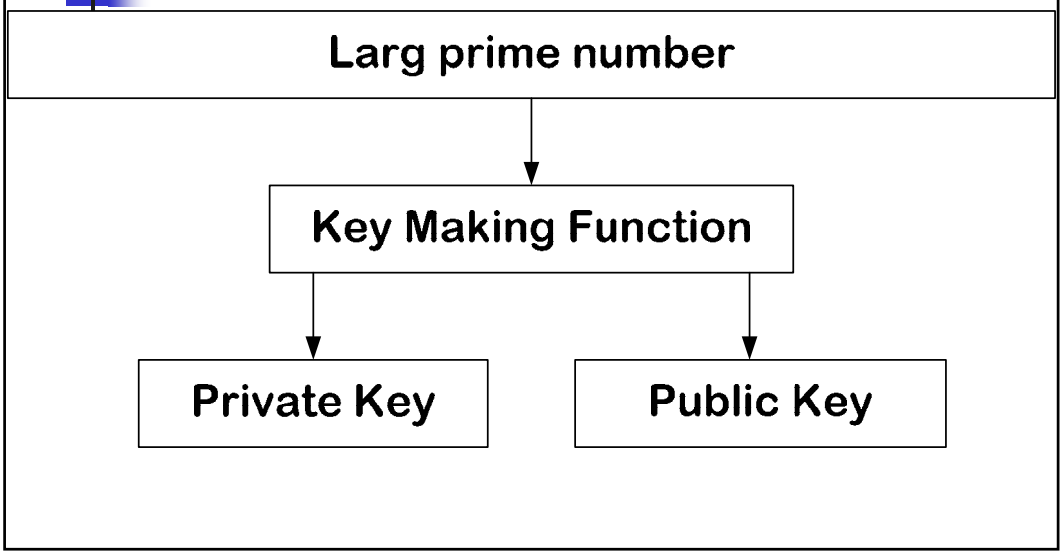
- In an asymmetric key system, Bob and Alice have separate padlocks.
  - First, Alice asks Bob to send his open padlock to her through regular mail, keeping his key.
  - When Alice receives it she uses it to lock a box containing her message, and sends the locked box to Bob.
  - Bob can then unlock the box with his key and read the message from Alice.
  - To reply, Bob must similarly get Alice's open padlock to lock the box before sending it back to her.

5

A postal analogy

- The critical advantage in an asymmetric key system is that Bob and Alice never need to send a copy of their keys to each other.
- This prevents a third party from copying a key while it is in transit,
- In addition, if Bob were to be careless and allow someone else to copy his key,
- Alice's messages to Bob would be compromised, but Alice's messages to other people would remain secret, since the other people would be providing different padlocks for Alice to use.

6



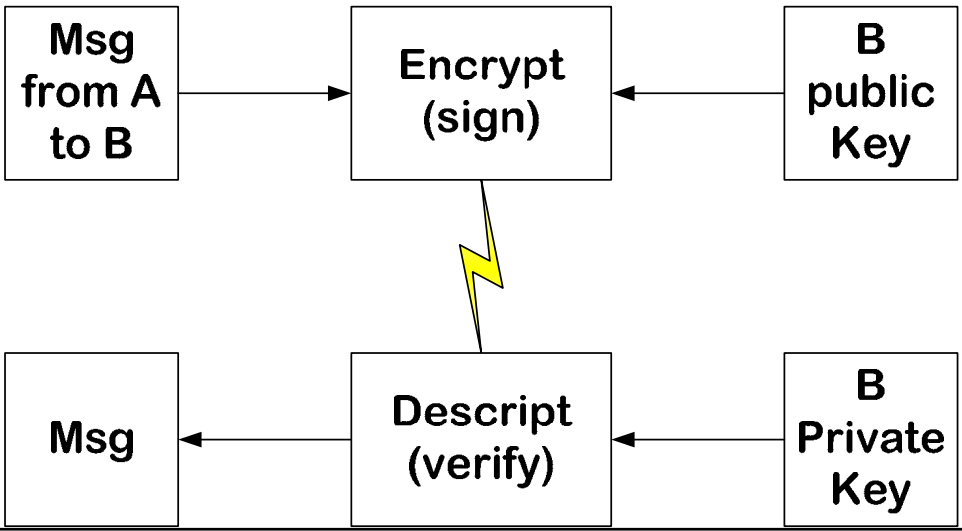
7

Public key cryptography

- The two main branches are:
  - Public key encryption — a message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key. This is used to ensure confidentiality.
  - Digital signatures — a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender signed it and that the message has not been tampered with. This is used to ensure authenticity.

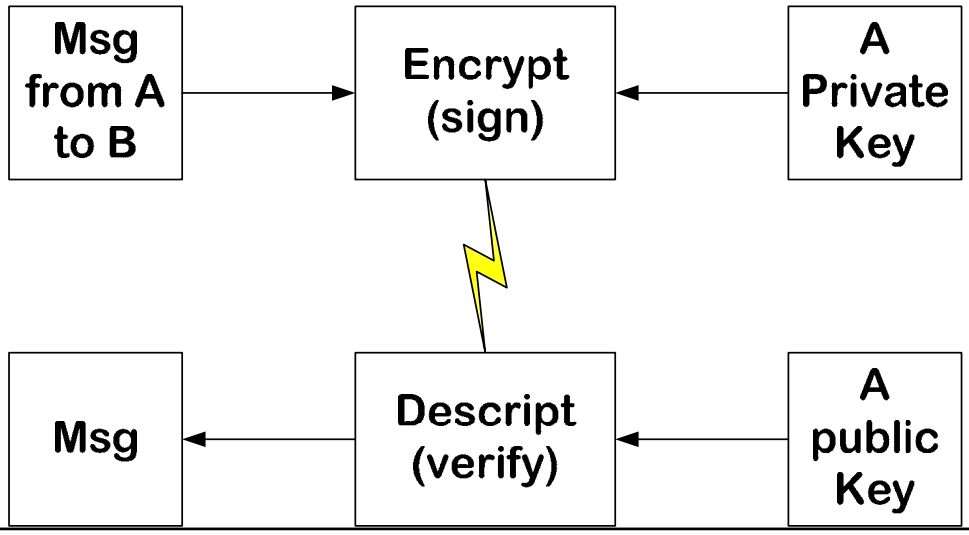
8

Public key encryption



9

Digital signatures

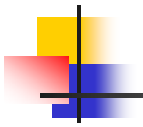


10

public-key encryption

- An analogy for public-key encryption is that of a locked mailbox with a mail slot.
- The mail slot is exposed and accessible to the public; its location (the street address) is in essence the public key.
- Anyone knowing the street address can go to the door and drop a written message through the slot; however, only the person who possesses the key can open the mailbox and read the message.

11



digital signatures

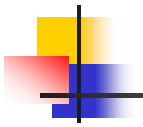
- An analogy for digital signatures is the sealing of an envelope with a personal wax seal.
- The message can be opened by anyone, but the presence of the seal authenticates the sender.

12

Public-key Problem

- A central problem for public-key cryptography is proving that a public key is authentic, and has not been tampered with or replaced by a malicious third party.
- The usual approach to this problem is to use a public-key infrastructure (PKI), in which one or more third parties, known as certificate authorities, certify ownership of key pairs.
- Another approach, used by PGP, is the "web of trust" method to ensure authenticity of key pairs.

13



Public key techniques

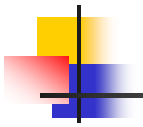
- Much more computationally intensive than purely symmetric algorithms.
- The judicious use of these techniques enables a wide variety of applications.
- In practice, public key cryptography is used in combination with secret-key methods for efficiency reasons.
- For encryption, the message may be encrypted with secret-key algorithm using a randomly generated key, and that key encrypted with the user's public key.

14

Public key techniques

- For digital signatures, a message is hashed (using a cryptographic hash function) and the smaller "hash value" is signed;
- Before verifying the signature, the recipient computes the hash of the message himself, and compares this hash value with the signed hash value to check that the message has not been tampered with.

15



Public key applications

- The most obvious application is confidentiality; a message which a sender encrypts using the recipient's public key can only be decrypted by the recipient's paired private key.
- Public-key digital signature algorithms can be used for sender authentication and non-repudiation.
  - For instance, a user can encrypt a message with his own private key and send it.
  - If another user can successfully decrypt it using the corresponding public key, this provides assurance that the first user (and no other) sent it.

16

Public key applications

- Cryptographic signature
  - a cryptographic hash value of the message is calculated, encrypted with the private key and sent with the message
  - The receiver can then verify message integrity and origin by calculating the hash value of the received message
  - The receiver need do decode the encrypted hash using the sender public key and compare it against the message hash
  - If the hash from the sender and the hash on the receiver side do not match, then the received message is not identical to the message which the sender "signed", or the sender's identity is wrong.

17

Public key applications

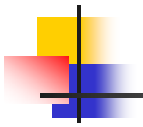
- Authentication, non-repudiation, and confidentiality,
  - The sender encrypt the message using his private key,
  - a second encryption is performed using the recipient's public key.
  - Receiver will decrypt the message with his private key
  - The ressult is decrypted using the sender public key
- Useful for many other applications, like digital cash, password-authenticated key agreement, multi-party key agreement, etc

18

Weaknesses

- Unfortunately, there is no public-key scheme with this property, since all public-key schemes are susceptible to brute force key search attack.
- Such attacks are impractical if the amount of computation needed to succeed (termed 'work factor' by Shannon) is out of reach of potential attackers.
- The work factor can be increased by simply choosing a longer key.
- Other attacks may be more efficient, and some are known for some public key encryption algorithms.

19



Weaknesses

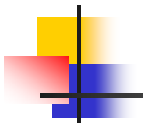
- Both RSA and ElGamal have known attacks which are much faster than the brute force approach
- Such estimates have changed both with the decreasing cost of computer power, and with new mathematical discoveries.
- In practice, these insecurities can be avoided by choosing key sizes large enough that the best known attack would take so long that it is not worth any adversary's time and money to break the code.
- For example, if an estimate to break an encryption scheme is one 100 years, and it were used to encrypt credit card details, they would be safe enough, since the time needed to decrypt the details will be rather longer than the useful life of those details

20

Weaknesses

- Typically, the key sizes needed are much longer for public key algorithms than for symmetric key algorithms.
- Major weaknesses have been found for several formerly promising asymmetric key algorithms.
- Recently, some attacks based on careful measurements of the exact amount of time it takes known hardware to encrypt plain text have been used to simplify the search for likely decryption keys (see side channel attack).
- Thus, mere use of asymmetric key algorithms does not ensure security; it is an area of active research to discover and protect against new and unexpected attacks.

21



Weaknesses

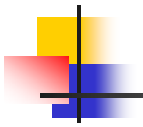
- Another potential security vulnerability in using asymmetric keys is the possibility of a man in the middle attack, in which communication of public keys is intercepted by a third party and modified to provide different public keys instead.
- Encrypted responses must also be intercepted, decrypted and re-encrypted by the attacker using the correct public key in all instances to avoid suspicion.
- This attack is difficult to implement in practice, but not impossible when using insecure media (e.g. public networks such the Internet or wireless communications).

22

Computational cost

- Most public key algorithms are relatively computationally costly in comparison with many symmetric key algorithms of apparently equivalent security.
- This has important implications for their practical use.
- Most are used in hybrid cryptosystems for efficiency; a shared secret key ("session key") is generated by one party and this much briefer session key is then encrypted by each recipient's public key.
- Each recipient uses the corresponding private key to decrypt the session key.
- Once all parties have obtained the session key they can use a much faster symmetric algorithm to encrypt and decrypt messages.

23



Algorithms

- Cramer-Shoup | DH | DSA | ECDH | ECDSA | EKE | ElGamal | GMR | IES | Lamport | MQV | NTRUEncrypt | NTRUSign | Paillier | Rabin | RSA | Schnorr | SPEKE | SRP | XTR