CS4331/CS5342 Network Security
Homework _2 Solution

Q.1. What are the pros and cons of public-key cryptography (5 points)

Ans: Public-key cryptography is a type of encryption that encrypts and decrypts data using two separate keys called public key and Private key.

Pros or Advantages:

- Easy key distribution
- No longer need to assume that Alice and Bob already share a secret.

Cons or Disadvantages:

- Much slower than symmetric-key cryptography
- Number theory calculations are much slower than XORs and bit-shifts.

Q.2. What are the properties of public key encryption? (5 points)

Ans:

- **Correctness:** Decrypting a ciphertext should result in the message that was originally encrypted
  Dec(*SK*, Enc(*PK*, *M*)) = *M* for all *PK*, *SK* ← KeyGen() and *M*
- **Efficiency:** Encryption/decryption should be fast
- **Security:** Alice (the challenger) just gives Eve (the adversary) the public key, and Eve doesn't request encryptions. Eve cannot guess out anything. Computationally infeasible to recover M with PK and ciphertext.

Q.3. Describe the steps of public key encryption with example (5 points)

Ans: Steps for Public key encryption:

Step1: Generate a pair of keys.

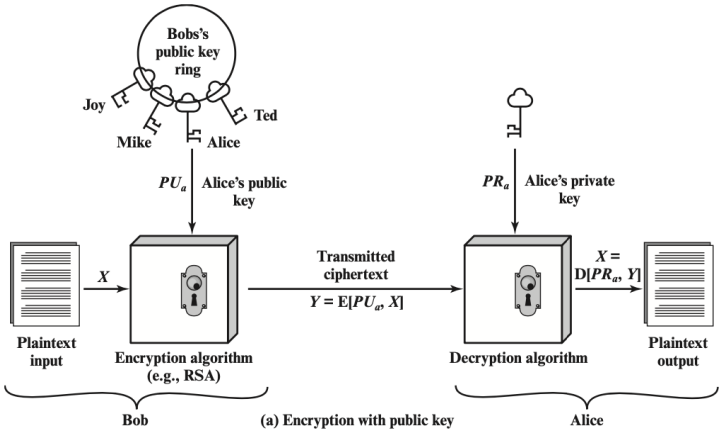
Step2:

- keep the private key / secret key (SK) and distribute the public key (PK).
- Place PK in a public register or other accessible file.

Step3: Bob encrypts the message with Alice's PK.

Step4: Upon receiving the ciphertext (CT), Alice decrypt CT with SK.

Example:



Q.4. Which categories should be used to classify public key cryptography algorithms? (5 points)

Ans: There are three categories used to classify Public key cryptography algorithms which are listed below:

1. **Encryption/Decryption**: It provides secrecy to the key.
2. **Digital signatures:** It provides authentication.
3. **Key exchange:** It consists of session keys.

- Some algorithms are suitable for all uses while the others are specific to one.
- Either of the two related keys can be used for encryption, with the other used for decryption.

Algorithm	Encryption/Decryption	Digital Signature	Key Exchange
RSA	Yes	Yes	Yes
Diffie–Hellman	No	No	Yes
DSS	No	Yes	No
Elliptic curve	Yes	Yes	Yes

Q.5. Write RSA encryption and decryption algorithms. Suppose the public key {e, n}, and private key {d,n} are given. **(5 points)**

Ans: RSA Encryption Algorithm:

Given a message M and a public key {e, n}, the RSA encryption algorithm works as follows:

1. Create an integer m from the message M such that $0 \leq m < n$.
2. Make the ciphertext c as $c \equiv m^e \pmod{n}$.
3. Return the ciphertext c.

RSA Decryption Algorithm:

Given a ciphertext c and a private key {d, n}, the RSA decryption algorithm works as follows:

1. Compute the plaintext p as $p \equiv c^d \pmod{n}$.
2. Convert the plaintext p back into the original message M.
   - It should be noted that step 2 of the RSA decryption process is required since it is possible that the plaintext p and the original message M are different.
   - Any encoding or formatting strategy that was employed to change M into m in the RSA encryption algorithm can be used to change p back into M.

Overall, the RSA encryption and decryption algorithms are relatively simple to implement and provide a high level of security for data transmission. However, the security of the algorithm relies on the difficulty of factoring large numbers, so it's important to use sufficiently large key sizes to prevent attacks.

Q.6. What are the possible attacks exploiting RSA's properties? **(5 points)**

Ans:

1. **Mathematical attacks**: Several approaches, all equivalent in effort to factoring the product of two primes. The defense against mathematical attacks is to use a large key size.
2. **Timing attacks**: These depend on the running time of the decryption algorithm.
3. **Chosen ciphertext attacks**: This type of attacks exploits properties of the RSA algorithm by selecting blocks of data. These attacks can be thwarted by suitable padding of the plaintext, such as PKCS1 V1.5 in SSL.

Q.7. What is meant by message authentication? (5 points)

Ans: Message authentication is concerned with:

1. Protecting the integrity of a message
2. Validating identity of originator
3. non-repudiation of origin (dispute resolution)

Q.8. What are the 4 approaches to achieve message authentication? (5 points)

Ans: Message authentication is the process of verifying the integrity and authenticity of a message. The 4 approaches to achieve message authentication are:

1. Message Encryption:

Message encryption by itself also provides a measure of authentication.

A. If symmetric encryption is used, then:
   1. Receiver knows sender that who must have created it.
   2. Since only sender and receiver know the key used.
   3. Known content cannot be altered.

B. If public-key encryption is used:
   1. Encryption provides no confidence of sender
   2. Since anyone potentially knows public key
   3. So, need to recognize corrupted messages

C. However, if
   1. Sender signs message using their private key
   2. Then encrypts with recipients' public key
   3. Have both secrecy and authentication

But at cost of two public-key uses on message

2. Message Authentication Codes (MACs):

A MAC is a cryptographic technique that uses a secret key to generate a tag that is appended to the message. The recipient can verify the integrity of the message by recalculating the tag using the same key and comparing it with the received tag.

3. Hash Function:

A Hash function is any function that can be used to map data of arbitrary size to fixed -size values, A secure hash function satisfies .

4. Digital Signatures:

A digital signature is a cryptographic technique that uses a private key to generate a signature that is attached to the message. The recipient can verify the authenticity and integrity of the message by using the corresponding public key to verify the signature.

Q.2. Short answer Questions (10points)

1. _____ encryption is a form of cryptosystem in which encryption and decryption are performed using a public key and a private key.
2. Asymmetric encryption transform plaintext to ciphertext using _____
3. Asymmetric encryption transforms plaintext into signature using_____
4. Public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to _____ encryption, which uses only one key.
5. Message authentication is a mechanism or service used to verify the _____ of a message.

Answers:

1. Asymmetric
2. Public Key
3. Private Key
4. symmetric
5. Integrity