Engineering Mathematics IV

UNIT IV
Learning Material

Unit – IV

Syllabus: Public-Key Cryptography

Public Key Cryptography: Principles of Public-Key Cryptosystems, The RSA Algorithm, Diffie-Hellman Key Exchange- The Algorithm, Key Exchange Protocols, Man-in-the-Middle Attack.

Terminology Related to Asymmetric Encryption:

- Asymmetric Keys
  - Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.
- Public Key Certificate
  - A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the corresponding private key.
- Public Key (Asymmetric) Cryptographic Algorithm
  - A cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.
- Public Key Infrastructure (PKI)
  - A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

3.1 Principles of public key cryptosystems

Asymmetric encryption is a form of cryptosystem in which encryption and decryption are performed using the different keys—one a public key and one a private key. It is also known as public-key encryption.

Public-key encryption scheme has six ingredients:

Plaintext: This is the readable message or data that is fed into the algorithm as input.

Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.

Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.

Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

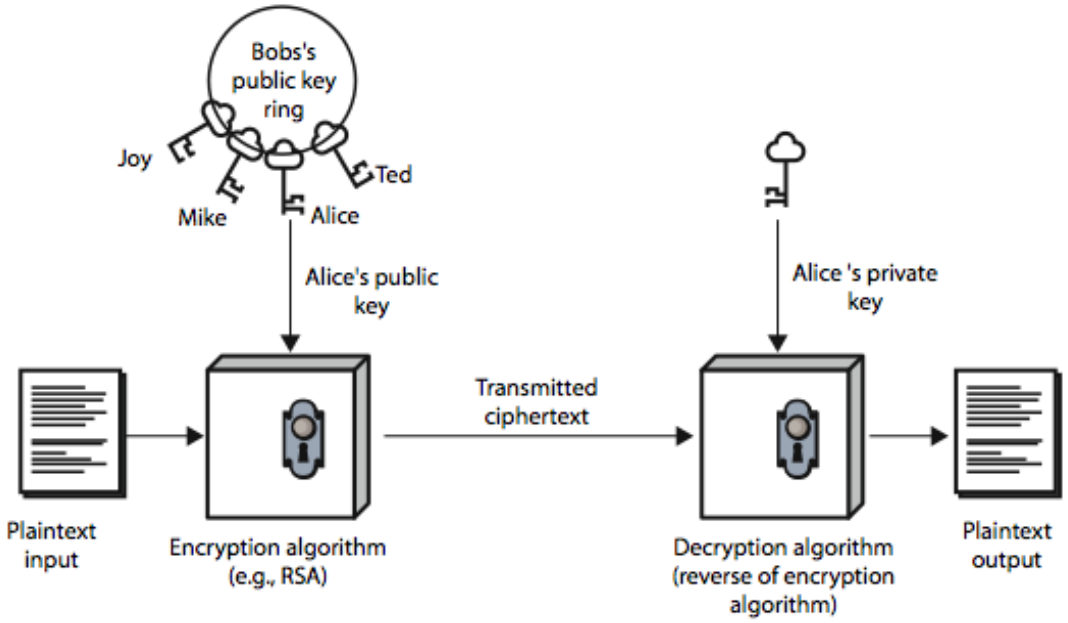
Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Conventional Vs. Public-Key Encryption

Conventional Encryption	**Public-Key Encryption**
Needed to Work:	**Needed to Work:**
The same algorithm with the same key is used for encryption and decryption.	One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
The sender and receiver must share the algorithm and the key.	The sender and receiver must each have one of the matched pair of keys (not the same one).
Needed for Security:	**Needed for Security:**
The key must be kept secret.	One of the two keys must be kept secret.
It must be impossible or at least impractical to decipher a message if no other information is available.	It must be impossible or at least impractical to decipher a message if no other information is available.
Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Requirements for Public-Key Cryptography

1. It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext: $C = E(PU_b, M)$
3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message: $M = D(_{PRb}, C) = D[PR_b, E(PU_b, M)]$
4. It is computationally infeasible for an adversary, knowing the public key, PU_b, to determine the private key, PR_b.
5. It is computationally infeasible for an adversary, knowing the public key, PU_b, and a ciphertext, C, to recover the original message, M.
6. The two keys can be applied in either order: $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$



(a) Encryption

3.2 RSA Algorithm

- Rivest-Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key encryption.
- The RSA scheme is a block cipher in which the plaintext and ciphertext are integers between 0 and n - 1 for some n.
- Typical size for n is 1024 bits, or 309 decimal digits. That is, n is less than 2^{1024}.
- Encryption and decryption are as follows:
  - for plaintext block M and ciphertext block C,
  - $C = M^e \bmod n$
  - $M = C^d \bmod n$
  - sender and receiver must know the value of n
  - The sender knows the value of e, and only the receiver knows the value of d.
  - This is a public-key encryption algorithm with a public key of PU = {e, n} and a private key of PR = {d, n}.
  - the following requirements are must:
    - It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all M < n.
    - It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of M < n.
    - It is infeasible to determine d given e and n.
  -

RSA Key Setup

- Each user generates a public/private key pair by:
- select two large primes at random - p, q
- compute their system modulus n= p * q
  - note ø(n) = ø(pq) = (p-1)(q-1)
- select the encryption key e
  - where $1<e<ø(n)$, $gcd(e,ø(n))=1$
- solve following equation to find decryption key d
  - $ed=1 \bmod ø(n)$ and $0 \le d \le N$
- publish their public encryption key: PU={e,n}
- keep secret private decryption key: PR={d,n}

RSA Use

- to encrypt a message M the sender:
  - obtains public key of recipient KU={e,N}
  - computes: C=Me mod N, where 0≤M<N
- to decrypt the ciphertext C the owner:
  - uses their private key PR={d,n}
  - computes: M=Cd mod N
- note that the message M must be smaller than the modulus N (block if needed)

RSA Key Generation

- users of RSA must:
  - determine two primes at random - p, q
  - select either e or d and compute the other
- primes p,q must not be easily derived from modulus N=p.q
  - means must be sufficiently large
  - typically guess and use probabilistic test
- exponents e, d are inverses, so use Inverse algorithm to compute the other

Primitive Root

- A primitive root of a prime number p is one whose powers modulo generate all the integers from 1 to p-1.
- If 'a' is a primitive root of the prime number 'p', then the numbers
  a mod p, a^2 mod p, …… , a^{p-1} mod p
  are distinct and consist of the integers from 1 through p-1 in some permutation.

3.3 Diffie-Hellman Key Exchange

- The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.
- Global Public Elements
  - q prime number
  - choose α such that α < q and α a primitive root of q
- User A Key Generation
  - Select private X_A such that $X_A < q$
  - Calculate public Y_A $Y_A = \alpha^{(X_A)} \bmod q$

- User B Key Generation
  - Select private X_B such that $X_B < q$
  - Calculate public Y_B $Y_B = \alpha^{(X_B)} \bmod q$
- Calculation of Secret Key by User A
  - $K = (Y_B)^{X_A} \bmod q$
- Calculation of Secret Key by User B
  - $K = (Y_A)^{X_B} \bmod q$

Man-in-the-Middle Attack

The Diffie-Hellman Algorithm is insecure against a man-in-the-middle attack. Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows:

1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys $Y_{D1}$and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates
$K_2 = (Y_A)^{X_{D2}} \bmod q$.
4. Bob receives $Y_{D1}$and calculates $K_1 = (Y_{D1})^{X_B} \bmod q$.
5. Bob transmits Y_B to Alice.
6. Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates
$K_1 = (Y_B)^{X_{D1}} \bmod q$.
7. Alice receives Y_{D2} and calculates $K_2 = (Y_{D2})^{X_A} \bmod q$.

The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates;

Assignment-Cum- Tutorial Questions

A) Objective Questions

1. Asymmetric encryption uses _____ keys.
   a. One b. two c. more than two
2. In _____ process the two communicating sides cooperate to exchange a session key
3. Signing (Digital Signatures) is achieved by _____ algorithms applied to the message.
4. In RSA algorithm the plaintext and ciphertext are _____
5. RSA algorithm is _____ cipher
   a. Block b. Stream
6. "p", "q" in RSA algorithm are to be _____ number
   a. composite b. prime c. integers d. imaginary
7. The purpose of Diffie-Hellman public-key cryptography is _____
   a. Encryption b. key exchange c. digital signatures
8. The security of Diffie-Hellman key exchange lies in usage of _____
9. What is the primitive root for 7? [ ]
   i. 2 b. 7 c. 3 d.5
10. In a RSA algorithm, say n is 33 and $\phi(n)=20$, what is the value of pair (p, q)?
    i. 11, 17 b. 3,5 c. 3,11 d. 33,1
11. If p=5, q=7 in RSA, then what is the value of e if d value is 13?
    i. 5 b. 6 c. 10 d. 2
12. Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows, Darth intercepts Y_A and transmits a public key Y_{D1} generated from random private key X_{D1} to Bob. This type of attack is called_____

i. Timing Attack b. Man-in-the-Middle Attack c. cryptanalysis d. Replay Attack.

13. 2 is the primitive root of _____

i. 6 b. 7 c. 11 d. 10

14. Bob is transmitting a message to Alice. Darth observes the running time taken for the decryption algorithm to crack it. What type of attack have Darth used?

a. timing attack b. brute force

b. c. mathematical attack d. chosen ciphertext attack

15. What is the value needed to calculate the key K value in Diffie-Hellman key exchange if "X_A" and "mod q" values are available?

a. private key of A b. Private key of B

c. public key of A d. public key of B

16. The Diffie-Hellman key exchange protocol is vulnerable to man-in-the-middle attack because of_____

a. no authentication of participants b. key size

c. primitive roots d. prime numbers

B) **Descriptive Questions**

1. **Describe a public-key cryptosystem with a neat sketch.**
2. **List and explain the requirements of Public-key Cryptography.**
3. **Explain the RSA Algorithm**
4. **What are three broad categories of applications of public-key cryptosystems?**
5. **Briefly explain Diffie-Hellman key exchange.**

6. **Perform encryption and decryption using RSA Algorithm for the following:**
    1. **p=3, q=13, e=5, M=10**
    2. **p=5, q=7, e=7, M=12**
7. **In a public-key system using RSA, say, you intercepted the cipher text C=8 sent to a user whose public key is e=13 and n=33. What is the plain text M?**
8. **Consider a Diffie-Hellman scheme with a common prime q=11 and a primitive root** $\alpha=2$.
    1. **show that 2 is a primitive root of 11**
    2. **If user A has public key** $Y_A=9$**, what is A's private key** X_A**?**
9. **Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q=7 and a primitive root** $\alpha=3$**, if Alice has a private key** $X_A=6$ **what is Alice's public key** Y_A**?**

C. Questions testing the analyzing/evaluating ability of students

1. Differentiate Conventional Encryption and Public-key Encryption.
2. In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant α^x mod q for some public number α.What would happen if the participants sent each x^α other for some public number α instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers? Explain.