CRYPTANALYSIS & CYBER DEFENSE
21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 17
PRINCIPLES OF PUBLIC KEY CRYPTO SYSTEMS

17.1 Aim

To fa7miliarize students with the basic concepts of Public-Key Cryptosystems and RSA algorithm.

17.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Public Key Cryptosystems. It also provides the necessary theoretical background and demonstrates the applications of public key cryptosystems.

17.3 Learning Outcomes

At the end of this session, students are expected to know

1. Define Public Key Cryptosystems
2. List out applications of Principles of Public Key Cryptosystems
3. Summarize Principles of Public Key Cryptosystems

17.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

17.5 Session Introduction

An overview of public-key cryptography is given in this session. The theory behind public-key cryptosystems is influenced by number theory. Public-key algorithms are not based on permutation and substitution, but rather on mathematical functions. In contrast to symmetric encryption, which employs just one key, public-key cryptography uses two different keys and is therefore asymmetric.

In terms of confidentiality, key distribution, and authentication, using two keys has significance.

17.6 Session Description

Public key cryptography is otherwise called as Asymmetric Encryption/Two-Key Encryption.

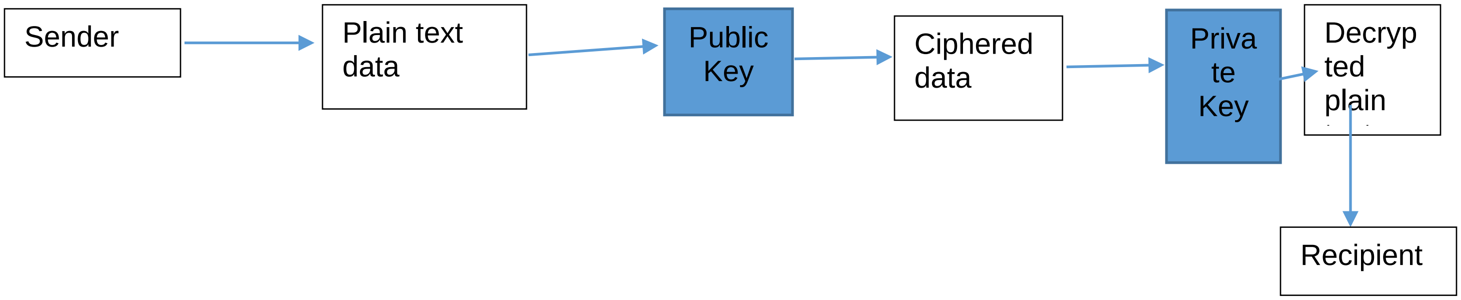


Figure 17.1 Public – Key Cryptography

Note: Copyrights of this diagram are reserved for the author of this diagram

Asymmetric key algorithms, which use a public key and a private key that are mathematically related to one another, are used in public key cryptography. The essential components of public key cryptography are as follows:

➢ **Public Key**:. This cryptographic key is one that is meant to be distributed to others. It is employed for digital signature verification and encryption. Anyone who wants to encrypt a message for the owner of the matching private key can do so by using the public key, which is freely distributable.

- **Private Key:** The owner keeps this secret key in strict confidence. Digital signatures and decryption are both accomplished using the private key. It must be kept secret and never disclosed to anyone else.
- **Key Generation Algorithm:** The public and private key pair are generated using a secure algorithm. The approach guarantees that the keys are mathematically connected but that it is computationally impossible to deduce one key from another.
- **Encryption Algorithm:** Plaintext messages are encrypted with the help of this algorithm and the public key. Only the associated private key can be used to decrypt the encrypted message.
- **Decryption Algorithm:** With the use of the private key, this procedure is used to decrypt the ciphertext and reveal the original plaintext message.

17.6.1 Public Key Cryptosystems for Confidentiality

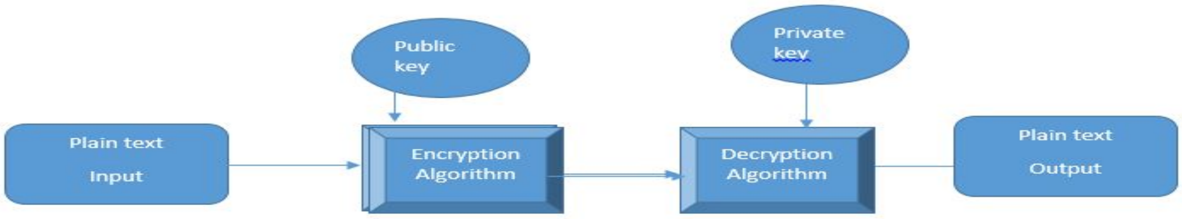


Figure 17.2 Encryption With Public Key of Destination: Confidentiality

Note: Copyrights of this diagram are reserved for the author of this diagram

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with public key of destination and destination decrypts the cipher-text with its own private key as private key of destination is only known to that destination no other entity will be able to decrypt the ciphertext and this is how the confidentiality of the message is preserved.

17.6.2 Public Key Cryptosystems for Authentication

Source and Destination generates a pair of keys by the name Public Key & Private

Keys. Source encrypts plaintext with private key of itself and destination decrypts the ciphertext with public key of source as private key of source is only known to that source no other entity will be able to encrypt or forge the plaintext and this is how the authentication of the message is preserved.

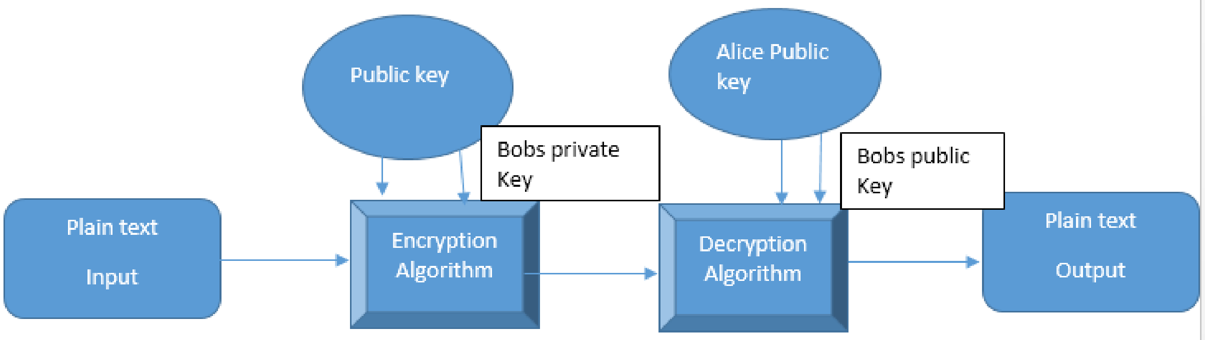


Figure 17.3 Encryption With Private Key of Source: Authentication

Note: Copyrights of this diagram are reserved for the author of this diagram

17.6.3 Public Key Cryptosystems for Confidentiality & Authentication

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with private key of itself and destination decrypts the ciphertext with public key of source as private key of source is only known to that source no other entity will be able to encrypt or forge the plaintext and this is how the authentication of the message is preserved.

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with public key of destination and destination decrypts the ciphertext with its own private key as private key of destination is only known to that destination no other entity will be able to decrypt the ciphertext and this is how the confidentiality of the message is preserved.

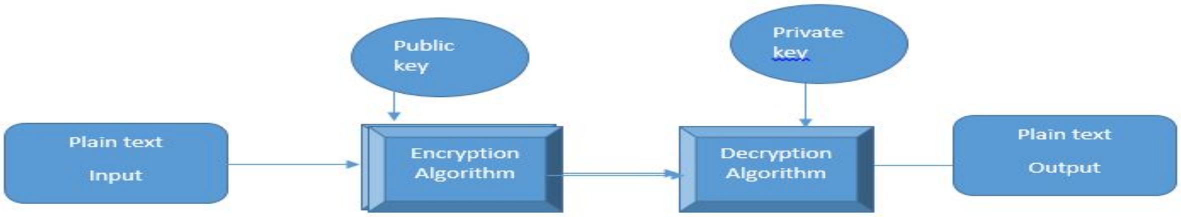
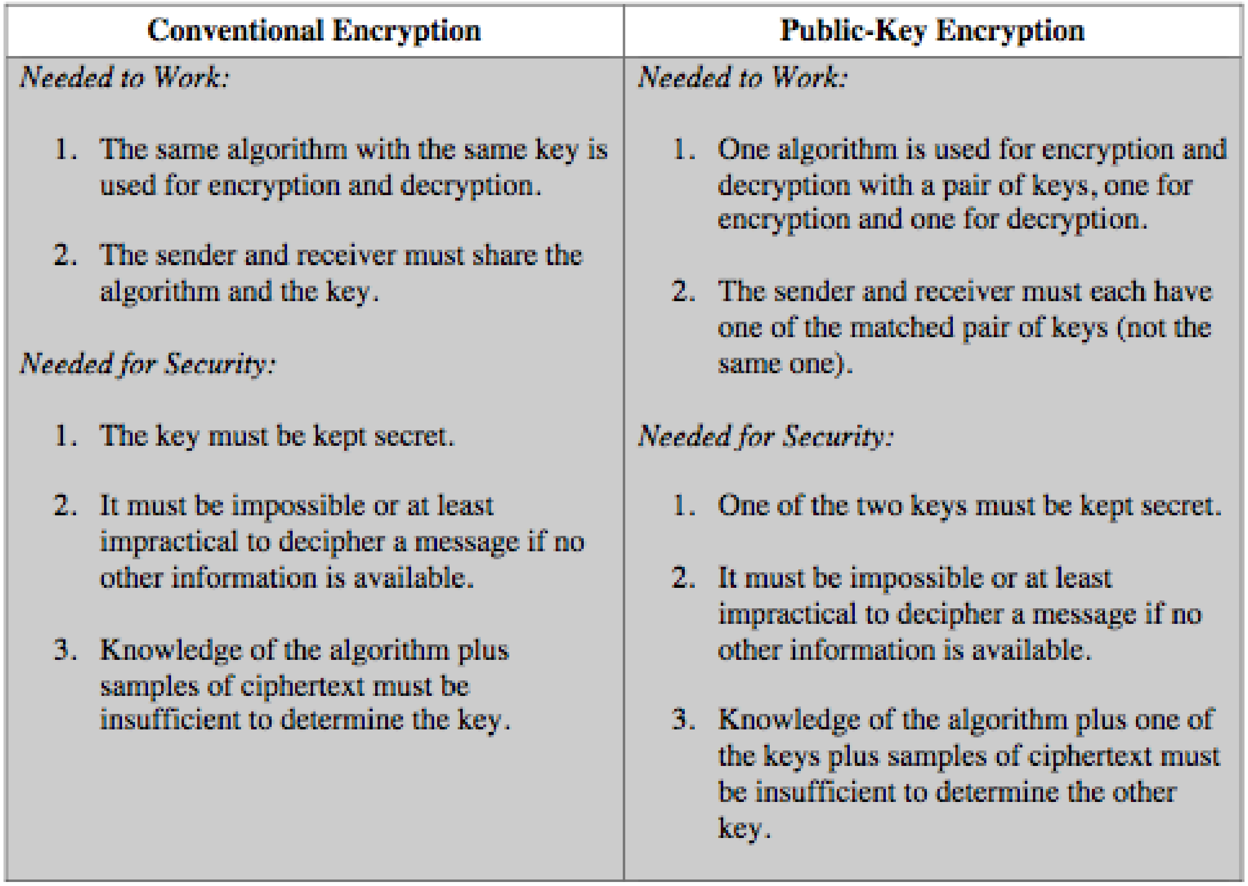


Figure 17.4 Encryption With Private Key of Source: Confidentiality & Authentication
Note: Copyrights of this diagram are reserved for the author of this diagram

17.6.4 Characteristics of Public Key Cryptography

- Despite the fact that the algorithm utilized and the public key are known (the public key is known to all entities involved in the communication). The private key should be computationally impossible to discover.
- It is computationally possible to encrypt plain text and decrypt cipher text if the encryption key and decryption key are available.
- In public key cryptography, each participant generates a pair of keys. The first is referred to as a Public Key, and the second as a Private Key. The reverse is also true: if a public key is used for encryption, a private key is utilized for decryption.

17.6.5 Comparison of Symmetric Key Cryptography & Public Key Cryptography



Conventional Encryption	Public-Key Encryption
Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key. *Needed for Security:* 1. The key must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.	*Needed to Work:* 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not the same one). *Needed for Security:* 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

Figure 17.5 Symmetric Encryption Vs Asymmetric Encryption
Note: Copyrights of this diagram are reserved for the author of this diagram

17.6.6 Applications of Public Key Cryptography:

- **Secure Communication**: Inorder to create secure communication channels over unreliable networks, such as the internet, public key cryptography is frequently utilized. It makes virtual private networks (VPNs), HTTPS-secured web browsing, and encrypted email exchange possible. Data is encrypted using the public key and decrypted using the private key to maintain confidentiality.
- **Digital Signatures:** Digital signatures are used to authenticate and add integrity to digital documents and messages, and public key cryptography makes it possible to create and verify them. A sender can sign the document using its private key and anyone with access to the sender's public key can check the signature to confirm the sender's identity and rule out any manipulation.
- **Key Exchange:** Public key cryptography facilitates secure key exchange between parties who have not previously communicated or shared a secret key. The Diffie-

Hellman key exchange protocol is a popular algorithm that allows two parties to agree upon a shared secret key over an insecure channel. This key can then be used for conventional encryption to secure subsequent communication.

17.7 Activities: NA

17.8 Examples: NA

17.9 Table Numbering: NA

17.10 Figures with Captions

17.11 Self Assessment Questions

1. Which of the following is a public key cryptosystem's main benefit over symmetric key cryptosystems?

a) Higher encryption speed

b) Smaller key sizes

c) Better resistsance to brute-force attacks

d) Simpler key management

2. What cryptographic technique is most frequently applied to public key encryption?

a) AES (Advanced Encryption Standard)

b) DES (Data Encryption Standard)

c) RSA (Rivest-Shamir-Adleman)

d) SHA-256 (Secure Hash Algorithm 256-bit)

3. What key is used for encryption in a public key cryptosystem?

a) Private key

b) Secret key

c) Public key

d) Session key

4. Which of the following is a prime example of a public key cryptosystem that is in broad use?

a) ElGamal

b) Triple DES

c) Blowfish

d) RC4

5. What key is utilized for decryption in a public key cryptosystem?

a) Private key

b) Secret key

c) Public key

d) Session key

6. What underlying mathematical issue underpins the security of numerous public key cryptosystems?

a) Integer factorization problem

b) Modular exponentiation problem

c) Discrete logarithm problem

d) Prime number generation problem

7. Which of the following is a public key cryptosystem application?

a) Digital signatures

b) Symmetric encryption

c) Hashing

d) Steganography

8. In a public key cryptosystem, which key is kept private?

a) Public key

b) Secret key

c) Private key

d) Session key

9. Which key in a public key cryptosystem is made available to others?

a) Public key

b) Secret key

c) Private key

d) Session key

10 Which of the following public key exchange protocols is most widely used?

a) SSL (Secure Sockets Layer)

b) IPsec (Internet Protocol Security)

c) PGP (Pretty Good Privacy)

d) HMAC (Hash-based Message Authentication Code)

11. Public-key cryptography is known as ?

a) Symmetric cryptography

b) Asymmetric cryptography

c) either a or b

d) None of the above

12. PKI stands for?

a) private key instance

b) private key infrastructure

c) public key instance

d) public key infrastructure

13. A communication is said to be insecure where data is transmitted in a manner that allows for interception also called?

a)attack

b)sniffing

c)ISP

d)citation

14. Knapsack problem can be solved by

a) Public key cryptosystem

b) Private key cryptosystem

c) Both a and b

d) Unique key cryptosystem

15. Confidentiality with asymmetric-key cryptosystem has its own

a) Entities

b) Data

c) Problems

d) Translator

16. Which of the following is a benefit of using public key cryptography?

a) It can be used to create digital signatures.

b) It can be used to encrypt and decrypt messages.

c) It can be used to create secure channels.

d) All of the above

17. Which of the following is a drawback of using public key cryptography?

a) It is not as secure as symmetric cryptography.

b) It is not widely supported.

c) It is computationally expensive.

d) None

18. Which of the following algorithms is used in public key cryptography?

a) RSA

b) Diffie-Hellman

c) Elliptic curve cryptography

d) All of the above

19. Which of the following is a one-way function?

a) A function that takes message as input and produces a variable-length output.

b) A function that takes message as input and produces a fixed-length output.

c) A function that is easy to compute but difficult to invert.

D) A function that is easy to compute and easy to invert.

20. Which of the following is a certificate authority?

a) A trusted third party that issues digital certificates.

b) A mathematical algorithm that allows a sender to sign a message so that the receiver can verify the sender's identity and the authenticity of the message.

c) A function that is easy to compute but difficult to invert.

d) A function that is difficult to compute but easy to invert.

17.12 Summary

Public key cryptography concepts are essential for enabling secure communication, digital information secrecy, integrity, authentication, and non-repudiation. In conclusion, symmetric encryption is faster and more effective than conventional encryption, but it does involve the safe exchange of a secret key. Although it is slower and more computationally expensive than symmetric encryption, asymmetric encryption offers a more secure method of key exchange and communication. Modern cryptographic systems and secure communication protocols use public key cryptography as a core building element because of its adaptability and robust security assurances. Although RSA is a strong encryption technique, it is important to keep in mind that the security of the method depends on the proper production and administration of keys, the use of appropriate key sizes, and defense against a variety of assaults such timing attacks and side-channel attacks.

17.13 Terminal Questions

1. Summarize Public key Cryptosystems
2. Distinguish Symmetric Encryption and Public key Cryptosystems
3. List Applications of Public key Cryptosystems
4. List Characteristics of Public key Cryptosystems.

17.14 Case studies: NA

17.15 Answer Key

Self-Assessment Questions

1. b) An asymmetric encryption algorithm

2. a) Encryption

3. b) Decryption

4. d) All of the above

5. d) Security level

6. a) Modular exponentiation

7. c) 256 bits

8. d) Factoring attacks

9. a) Integer factorization problem

10. c) PKCS#1 (Public Key Cryptography Standard

11. b) asymmetric cryptography

12. d) public key infrastructure

13. b)sniffing

14. a)Public key cryptosystem

15. c) Problems

16. d) All of the above

17. c) It is computationally expensive.

18. d)All of the above

19. c) A function that is easy to compute but difficult to invert.

20. a)A trusted third party that issues digital certificates.

Terminal Questions

1. ***Public Key Cryptosystems for Confidentiality***

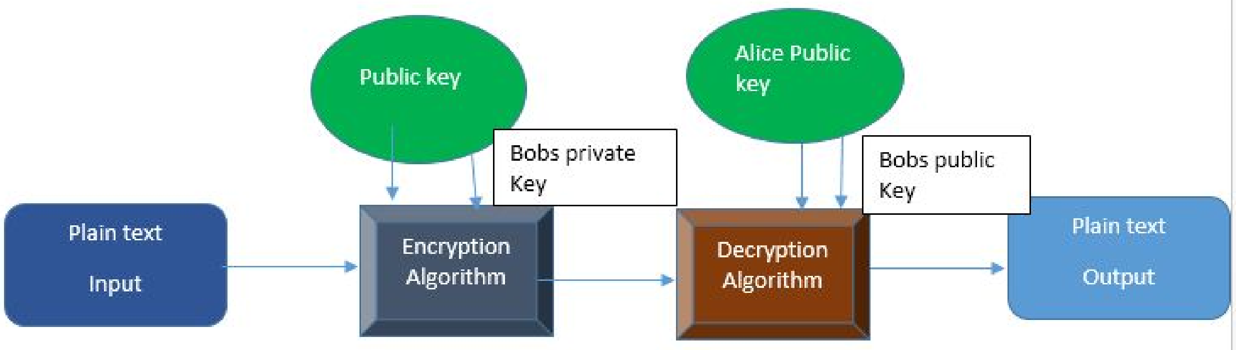


Figure: Encryption With Public Key of Destination: Confidentiality

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with public key of destination and destination decrypts the ciphertext with its own private key as private key of destination is only known to that destination no other entity will be able to decrypt the ciphertext and this is how the confidentiality of the message is preserved.

Public Key Cryptosystems for Authentication

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with private key of itself and destination decrypts the ciphertext with public key of source as private key of source is only known to that source no other entity will be able to encrypt or forge the plaintext and this is how the authentication of the message is preserved.

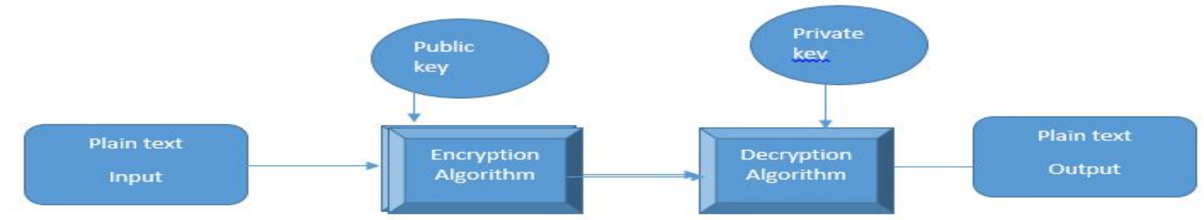
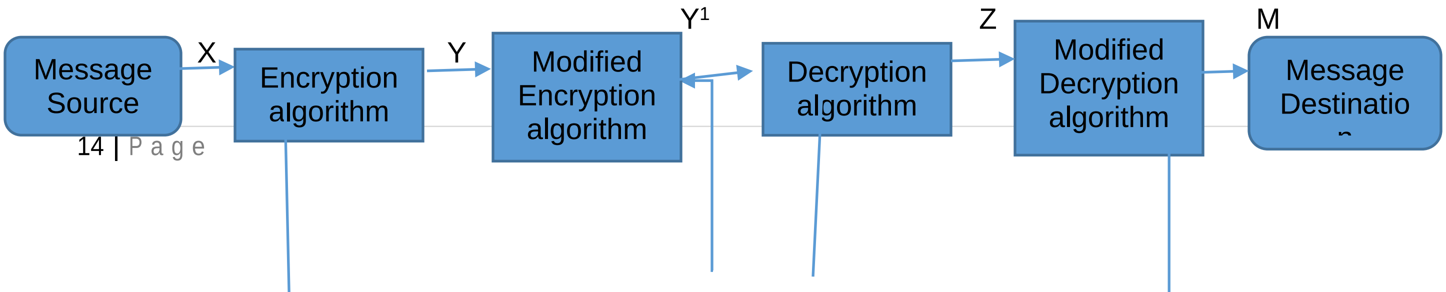


Figure Encryption With Private Key of Source: Authentication

Public Key Cryptosystems for Confidentiality & Authentication

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with private key of itself and destination decrypts the ciphertext with public key of source as private key of source is only known to that source no other entity will be able to encrypt or forge the plaintext and this is how the authentication of the message is preserved.

Source and Destination generates a pair of keys by the name Public Key & Private Keys. Source encrypts plaintext with public key of destination and destination decrypts the ciphertext with its own private key as private key of destination is only known to that destination no other entity will be able to decrypt the ciphertext and this is how the confidentiality of the message is preserved.



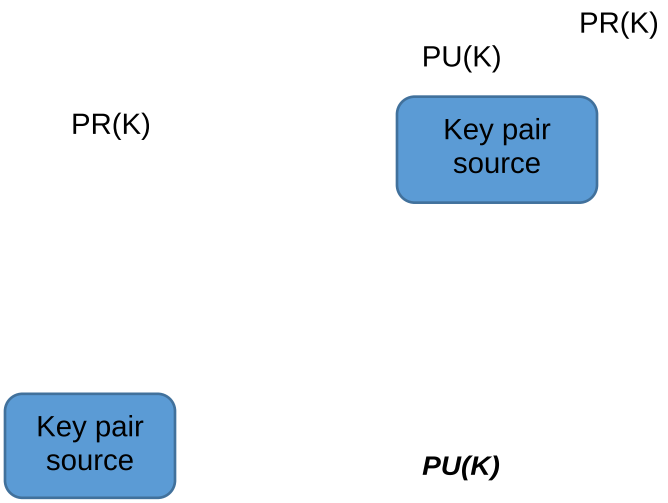


Figure 17.4 Encryption With Private Key of Source: Confidentiality & Authentication

2. Comparison of Symmetric Key Cryptography & Public Key Cryptography

Sr. No	Conventional Algorithm	Public Key Algorithm
1	**Needed to work** The same algorithm with the same key is used for encryption and decryption	**Needed to work** : one algorithm is used for encryption and decryption with a pair of key
2	**Needed to work** The sender and Receiver must share the algorithm and key	The sender and Receiver must each have one of the matched pair of keys(not the same one)
	Needed to Security	**Needed to Security**
3	The key must be Kept secret.	One of the two keys must be kept secret.
4	It must be impossible or atleast impractical to decipher a message if no other information is available.	It must be impossible or at least impractical to decipher a message if other message is available.
5	Knowledge of algorithm plus samples of cipher text must be insufficient to determine the key.	Knowledge of algorithm plus one of the keys plus samples of cipher text must be insufficient to determine the other key

3. Applications of Public Key Cryptography:

Secure Communication: Inorder to create secure communication channels over unreliable networks, such as the internet, public key cryptography is frequently utilized. It makes virtual private networks (VPNs), HTTPS-secured web browsing, and encrypted email exchange possible. Data is encrypted using the public key and decrypted using the private key to maintain confidentiality.

Digital Signatures: Digital signatures are used to authenticate and add integrity to digital documents and messages, and public key cryptography makes it possible to create and verify them. A sender can sign the document using its private key and anyone with access to the sender's public key can check the signature to confirm the sender's identity and rule out any manipulation.

Key Exchange: Public key cryptography facilitates secure key exchange between parties who have not previously communicated or shared a secret key. The Diffie-Hellman key exchange protocol is a popular algorithm that allows two parties to agree upon a shared secret key over an insecure channel. This key can then be used for conventional encryption to secure subsequent communication.

4. ***Characteristics of Public Key Cryptography***

- Despite the fact that the algorithm utilized and the public key are known (the public key is known to all entities involved in the communication). The private key should be computationally impossible to discover.
- It is computationally possible to encrypt plain text and decrypt cipher text if the encryption key and decryption key are available.
- In public key cryptography, each participant generates a pair of keys. The first is referred to as a Public Key, and the second as a Private Key. The reverse is also true: if a public key is used for encryption, a private key is utilized for decryption.

17.16 Glossary

GNFs-General Number Field Sieve

QS-Quadratic Sieve

RSA- Ron Rivest, Shammir, Adleman

VPN- Virtual Private Network

SSL/TLS – Secure Socket Layer

SSH-Secure Shell

CA-Certificate Authority

PGP-Pretty Good Privacy

17.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm's, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

17.18 Keywords

Public key cryptosystems, Asymmetric Encryption, RSA.

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 18

PRINCIPLES OF PUBLIC KEY CRYPTO SYSTEMS, RSA ALGORITHM

18.1 Aim

To fa7miliarize students with the basic concepts of Public-Key Cryptosystems and RSA algorithm.

18.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Public Key Cryptosystems and RSA Algorithm. It provides the necessary theoretical background and demonstrates the applications of public key cryptosystems. This session further allows students to apply RSA algorithm for various values of Plaintext and analyze attacks on RSA Algorithm.

18.3 Learning Outcomes

At the end of this session, students are expected to know

4. Apply RSA Algorithm for a given value of plaintext.
5. Summarize attacks on RSA Algorithm

18.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

18.5 Session Introduction

An overview of public-key cryptography is given in this session. The theory behind public-key cryptosystems is influenced by number theory. Public-key algorithms are not based on permutation and substitution, but rather on mathematical functions. In contrast to symmetric encryption, which employs just one key, public-key cryptography uses two different keys and is therefore asymmetric.

In terms of confidentiality, key distribution, and authentication, using two keys has significance. The RSA Algorithm is one such instance of a public-key cryptosystem.

18.6 Session Description

18.6.1 RSA Algorithm

It is a public key encryption algorithms. Ron Rivest, Adi Shamir, and Leonard Adleman, who introduced it in 1977. It is based on mathematical properties of modular exponentiation and the difficulty of factoring large composite numbers into their prime factors

Key Generation

Select two distinct prime numbers c and d

r=c*dwhich becomes the modulus for the RSA algorithm.

Find Euler's totient function φ(r),= (c-1)*(d-1)

Select f ; gcd(f, φ(r))=1

Encryption

Ciphertext C is computed as C = (M^f) mod r. Here, M represents the plaintext message.

Decryption

Plaintext M = (C^g) mod r. Here, C represents the ciphertext.

18.6.2 Attacks on RSA Algorithm

- **Brute Force:** Trying all possible private keys until the correct one is found. Brute-forcing RSA is computationally infeasible with current technology.
- **Factoring:**. The security provided by RSA is predicated on the notion that computing the prime factors of large numbers is computationally challenging. To effectively factor large numbers, there are a number of factoring algorithms available, including General Number Field Sieve (GNFS) and Quadratic Sieve (QS). A breakthrough in factoring could make RSA's security more vulnerable.
- **Timing Attacks:** Timing attacks take advantage of differences in how quickly cryptographic operations complete in order to retrieve sensitive data. An attacker may be able to determine information about the private key by meticulously calculating the time required for RSA operations. Timing attacks can be lessened by defenses like blindness and constant-time implementations.
- **Side-Channel Attacks:** The information that is revealed during the physical implementation of a cryptographic algorithm, such as power consumption, electromagnetic radiation, or acoustic emanations, is used in side-channel attacks. Techniques like power analysis, electromagnetic analysis, and fault attacks are examples of side-channel attacks. These attacks can be thwarted with the use of effective defenses like constant-time algorithms and secure hardware.

18.7 Activities (Problem Solving)

1. Generate the keys using the following values: c = 17, d= 11, f= 7 and encrypt plaintext M=9 using RSA algorithm.

2. Generate the keys using the following values: c = 61, d = 53, f = 17 and encrypt plaintext M=9 using RSA algorithm.

18.8 Examples

Generate the keys using the following values: c = 13, d= 17, f= 7 and encrypt plaintext
M=9 using RSA algorithm.

Two distinct prime numbers c=13 and d=17

r=c*d= 13*17= 221

Find Euler's totient function $\varphi(r)=(c-1)*(d-1)=(13-1)*(17-1)=12*16=192$

Select f ; $\gcd(f, 192)=1$ so $f=7$

Find g ; $(g * f) \bmod \varphi(r) = 1$ $(g*7) \bmod 192=1$ means $g=55$

.Encryption

Plaintext M=7

Ciphertext $C = (M^f) \bmod r$.

$C=(7^7) \bmod 221 = 196$

Decryption

Plaintext $M = (C^g) \bmod r$.

$M = (196^{55}) \bmod 221 =7$

18.9 Table Numbering: NA

18.10 Figures with Captions: NA

18.11 Self Assessment Questions

1. Expand RSA?

a) A symmetric encryption algorithm

b) An asymmetric encryption algorithm

c) A hashing algorithm

d) A key exchange protocol

2. Public Key in RSA is used for

a) Encryption

b) Decryption

c) Digital signature generation

d) Key exchange

3. Private Key in RSA is used for

a) Encryption

b) Decryption

c) Digital signature generation

d) Key exchange

4. Identify necessary step in generating an RSA key pair

a) Generating two large prime numbers

b) Computing the modular inverse

c) Calculating the Euler's totient function

d) All of the above

5. What is the size of the modulus in an RSA key pair IS directly proportional to?

a) Encryption speed

b) Decryption speed

c) Key generation time

d) Security level

6. Identify computationally expensive in RSA

a) Modular exponentiation

b) Modular multiplication

c) Modular addition

d) Modular subtraction

7. In RSA, what is the recommended length for the public modulus (in bits) for secure communication?

a) 64 bits

b) 128 bits

c) 256 bits

d) 512 bits

8. What is the primary weakness of RSA when using small or weak keys?

a) Brute-force attacks

b) Frequency analysis attacks

c) Man-in-the-middle attacks

d) Factoring attacks

9. Which cryptographic problem does RSA rely on for its security?

a) Integer factorization problem

b) Discrete logarithm problem

c) Prime number generation problem

d) Modular exponentiation problem

10. What is the standard padding scheme used in RSA to prevent certain attacks?

a) ECB (Electronic Code Book)

b) CBC (Cipher Block Chaining)

c) PKCS#1 (Public Key Cryptography Standard #1)

d) ANSI X9.31

11. What is the mathematical relationship between the public key and the private key in the RSA algorithm?

a) The public key is the inverse of the private key

b) The public key is the square root of the private key

c) The public key is the product of the private key and a prime number

d) The public key is the sum of the private key and a prime number

12. Which of the following is not a property of the RSA algorithm?

a) It is an asymmetric cryptography algorithm

b) It is a secure algorithm

c) It is a fast algorithm

d) It is a scalable algorithm

13.In RSA, Φ(n) = _______ in terms of p and q.

a) (p)/(q)

b) (p)(q)

c) (p-1)(q-1)

d) (p+1)(q+1)

14.For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text.

a) C=80

b) C=92

c) C=56

d) C=23

15.What is the purpose of the modulus in the RSA algorithm?

a) To encrypt data

b) To decrypt data

c) To generate the public key

d) To generate the private key

16.What is the purpose of the exponent in the RSA algorithm

a) To encrypt data

b) To decrypt data

c) To generate the public key

d) To generate the private key

17.What is the difference between the RSA algorithm and the Diffie-Hellman algorithm?

a) The RSA algorithm is asymmetric, while the Diffie-Hellman algorithm is symmetric

b) The RSA algorithm is slower, while the Diffie-Hellman algorithm is faster

c) The RSA algorithm is more secure, while the Diffie-Hellman algorithm is less secure

d) The RSA algorithm is used for encryption, while the Diffie-Hellman algorithm is used for key exchange

18. What is the largest RSA key size that has been used in practice?

a) 2048 bits

b) 4096 bits

c) 8192 bits

d) 16384 bits

19. What is the future of the RSA algorithm?

a) The RSA algorithm will be replaced by a more secure algorithm

b) The RSA algorithm will be used alongside other algorithms for encryption

c) The RSA algorithm will be used for key exchange

d) The RSA algorithm will be used for digital signatures

20.What is the smallest RSA key size that is considered secure?

a) 1024 bits

b) 2048 bits

c) 4096 bits

d) 8192 bits

18.12 Summary

Public key cryptography concepts are essential for enabling secure communication, digital information secrecy, integrity, authentication, and non-repudiation. In conclusion, symmetric encryption is faster and more effective than conventional encryption, but it does involve the safe exchange of a secret key. Although it is slower and more computationally expensive than symmetric encryption, asymmetric encryption offers a more secure method of key exchange and communication. Modern cryptographic systems and secure communication protocols use public key cryptography as a core building element because of its adaptability and robust security assurances. Although RSA is a strong encryption technique, it is important to keep in mind that the security of the method depends on the proper production and administration of keys, the use of appropriate key sizes, and defense against a variety of assaults such timing attacks and side-channel attacks.

18.13 Terminal Questions

1. Summarize RSA Algsorithm.

2. Perform encryption and decryption using the RSA algorithm for the following: c = 3; d = 11, f = 7; M = 5.

3. Analyze attacks on RSA Algorithm**.**

18.14 Case studies: NA

18.15 Answer Key

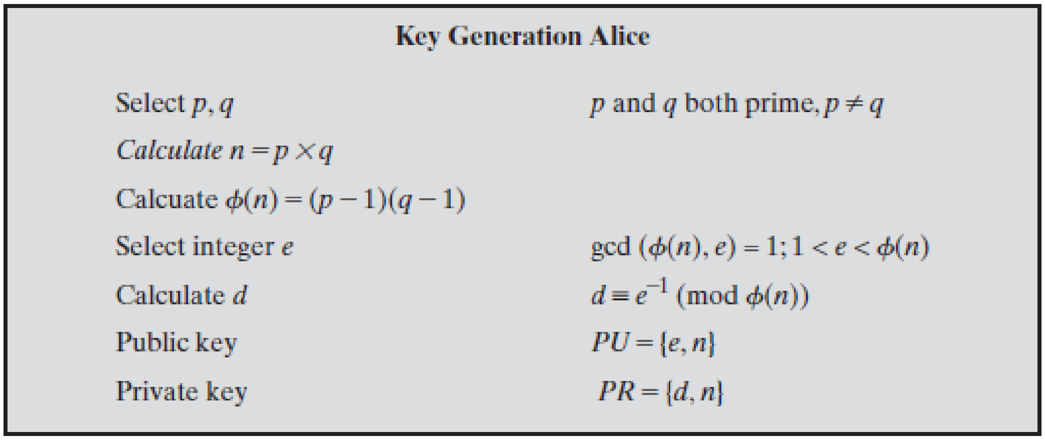
Self-Assessment Questions

1. c) Better resistance to brute-force attacks
2. c) RSA (Rivest-Shamir-Adleman)
3. c) Public key
4. a) ElGamal
5. a) Private key
6. c) Discrete logarithm problem
7. a) Digital signatures
8. c) Private key
9. a) Public key

10. a) SSL (Secure Sockets Layer)
11. a) The public key is the inverse of the private key
12. c) It is a fast algorithm
13. c) (p-1)(q-1)
14. a) C=80
15. d) To generate the private key
16. a) To encrypt data
17. d) The RSA algorithm is used for encryption, while the Diffie-Hellman algorithm is used for key exchange
18. c) 8192 bits
19. b) The RSA algorithm will be used alongside other algorithms for Encryption
20. b) 2048 bits

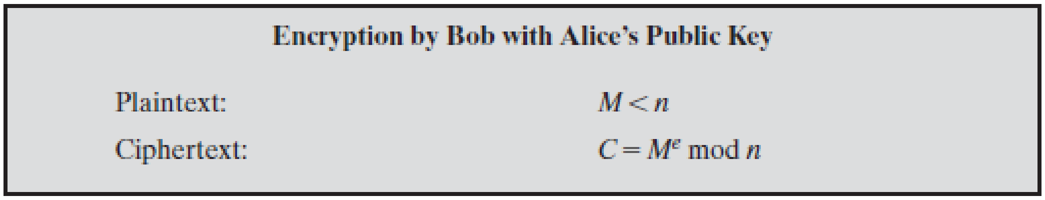
Terminal Questions

5. RSA Algorithm



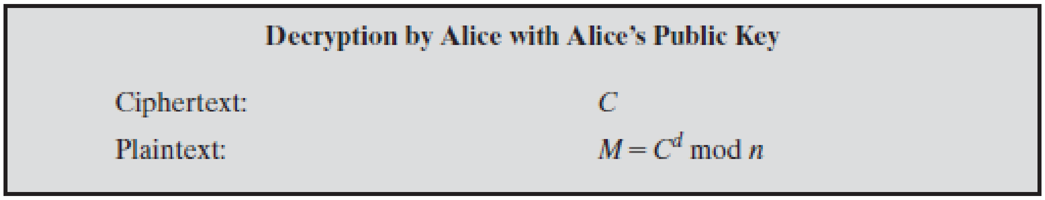
Key Generation Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$



Encryption by Bob with Alice's Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$



Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

2.

Calculate n: r = c * d = 3 * 11 = 33

Calculate φ: φ = (c - 1) * (d - 1) = (3 - 1) * (11 - 1) = 2 * 10 = 20

Public key exponent (f): Given as f = 7

Private key exponent (g): Given as g = 31

Encryption: C = M^f (mod r) = 5^7 (mod 33) = 16807 (mod 33) = 19

Decryption: M = C^g (mod r) = 19^31 (mod 33) ≈ 5

Therefore, the encrypted ciphertext (C) is 19, and the decrypted plaintext (M) is 5.

3.Attacks on RSA Algorithm

- **Brute Force:** Trying all possible private keys until the correct one is found. Brute-forcing RSA is computationally infeasible with current technology.
- **Factoring:**. The security provided by RSA is predicated on the notion that

computing the prime factors of large numbers is computationally challenging. To effectively factor large numbers, there are a number of factoring algorithms available, including General Number Field Sieve (GNFS) and Quadratic Sieve (QS). A breakthrough in factoring could make RSA's security more vulnerable.

- **Timing Attacks:** Timing attacks take advantage of differences in how quickly cryptographic operations complete in order to retrieve sensitive data. An attacker may be able to determine information about the private key by meticulously calculating the time required for RSA operations. Timing attacks can be lessened by defenses like blindness and constant-time implementations.
- **Side-Channel Attacks:** The information that is revealed during the physical implementation of a cryptographic algorithm, such as power consumption, electromagnetic radiation, or acoustic emanations, is used in side-channel attacks. Techniques like power analysis, electromagnetic analysis, and fault attacks are examples of side-channel attacks. These attacks can be thwarted with the use of effective defenses like constant-time algorithms and secure hardware.

18.16 Glossary

GNFs-General Number Field Sieve

QS-Quadratic Sieve

RSA- Ron Rivest, Shammir, Adleman

VPN- Virtual Private Network

SSL/TLS – Secure Socket Layer

SSH-Secure Shell

CA-Certificate Authority

PGP-Pretty Good Privacy

18.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm’s, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011
4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

18.18 Keywords

Public key cryptosystems, Asymmetric Encryption, RSA.

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 19

DIFFIE-HELMAN KEY EXCHANGE ALGORITHM

19.1 Aim

To familiarize students with the basic concept of Diffie-Hellman Algorithm

19.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Diffie-Hellman Key Exchange Algorithm. It provides the necessary theoretical background and demonstrates how a secret key is exchanged between source and destinations. This session further allows students to apply Diffie-Hellman Key Exchange Algorithm for various values of Plaintext and analyze attack on Diffie-Hellman Key Exchange Algorithm.

19.3 Learning Outcomes

At the end of this session, students are expected to know

1. Apply Diffie-Hellman Key Exchange Algorithm to generate plaintexts.
2. Summarize Man-in-the-Middle attack on Diffie-Hellman Algorithm

19.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

19.5 Session Introduction

In this session, we will explore the fundamentals of public-key cryptography. The underlying principles of public-key cryptosystems are grounded in number theory, making use of mathematical functions rather than substitution and permutation techniques. Unlike symmetric encryption, which relies on a single key, public-key cryptography employs two distinct keys, giving rise to various implications for confidentiality, key distribution, and authentication. One prominent example of public-key cryptosystems that we will delve into is the Diffie-Hellman algorithm,

19.6 Session Description

19.6.1 Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman key exchange algorithm is a protocol created to make it easier for two parties to establish a shared secret key via an unreliable channel. This algorithm was created by Whitfield Diffie and Martin Hellman in 1976 and is based on the idea of discrete logarithms. Its main benefit is that it makes it possible for two parties—typically referred to as Alice and Bob—to agree on a secret key without actually communicating it

- **Setup:**

Alice and Bob together must choose a prime number C a primitive root modulo often denoted as "D." These values are publicly known.

They also choose their own private keys: Alice selects "E," and Bob selects "F." These private keys are kept secret.

- **Key Generation:**

Alice computes her public key by calculating "A = D^E mod C" and sends it to Bob. Bob computes his public key by calculating "B = D^F mod C" and sends it to Alice.

- **Shared Secret Calculation:**

Alice computes the shared secret key using the formula "S = B^E mod C."

Bob computes the shared secret key using the formula "S = A^F mod C."

- **Shared Secret Exchange:**

After performing the calculations, both Alice and Bob have arrived at the same shared secret key, "s." This key can now be used for secure communication

19.6.2***Mathematical Proof that a Secret Key is Exchanged by source & Destination in Diffie-Hellman Key Exchange Algorithm***

S = A^F mod C //Secret Key of Bob//

=(D^E mod C) ^F mod p // B is Public key of Bob//

=(D^E)^F mod C // by the rules of modular arithmetic//

= D^E^F mod C

= D^F^E mod C

= (D^F mod C) ^E mod p

= (D^F) ^E mod C

= B^E mod C // Secret Key of Alice//

19.6.3 Man-in-the-Middle Attack (MITM)

A man-in-the-middle (MITM) attack is a sort of cyberattack in which an attacker secretly intercepts and maybe modifies the communication between two parties who they perceive to be directly speaking with one another. While actually controlling and manipulating the communication, the attacker places himself in the way of the two parties, giving the impression that they are speaking directly to one another.

An example of a man-in-the-middle attack would be as follows:

Intercepting Communication:

In this scenario, an unauthorized individual intercepts the communication between Party A and Party B. This interception can occur through physical means or by exploiting weaknesses within the network or communication channels.

Impersonation:

In this situation, the attacker assumes the identity of Party A when communicating with Party B, establishing a connection between themselves and Party B. Simultaneously, the attacker also impersonates Party B when communicating with Party A, establishing a separate connection between themselves and Party A.

Relay and Alteration:

Now, the attacker gains the ability to intercept and manipulate the communication between

Party A and Party B. They have the option to passively eavesdrop on the conversation, listening in without altering the content, or they can take an active role by modifying the messages exchanged between the two parties.

Intercepted Data between Party A and Party B. This can include confidential data, login credentials, financial information, or personal details.

In terms of manipulation, the attacker has the potential to alter the communication by injecting malicious content or commands. They can redirect the communication to their own systems or modify the messages to deceive the parties involved.

Concealment:

The attacker's objective is to maintain stealth during the attack, ensuring that neither Party A nor Party B detects their presence or manipulation of the communication. Their goal is to remain undetected throughout the process, increasing their chances of exploiting the situation for their benefit.

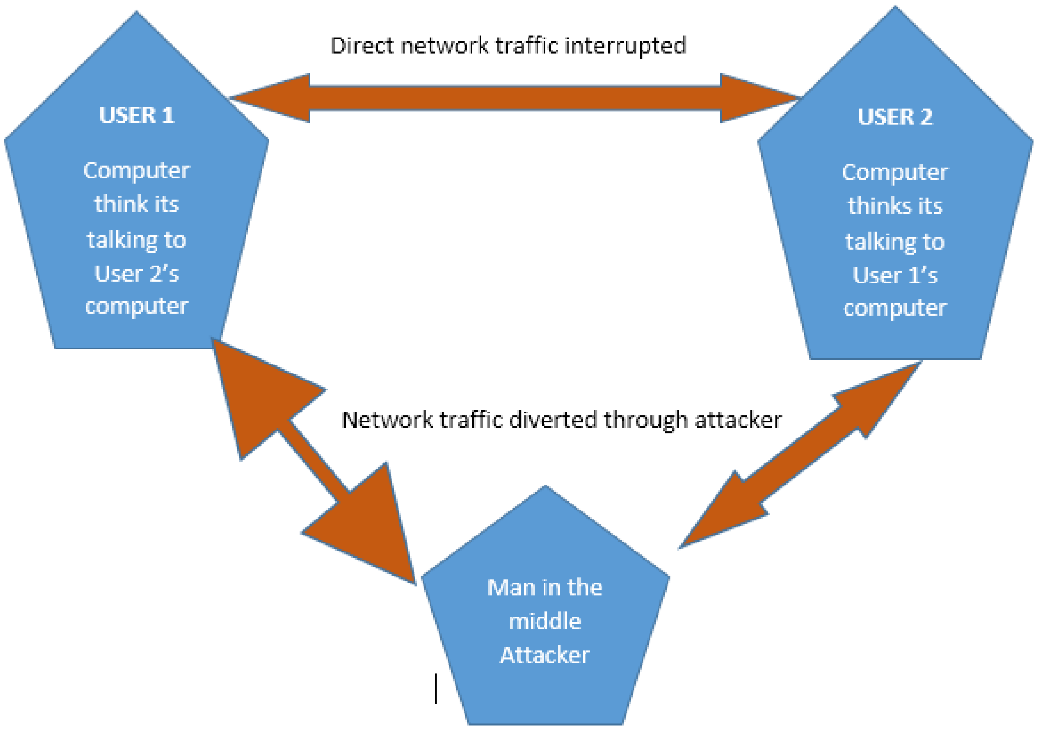

Direct network traffic interrupted
USER 1
Computer think its talking to User 2's computer
USER 2
Computer thinks its talking to User 1's computer
Network traffic diverted through attacker
Man in the middle Attacker

Figure 19.1 ***Man-in-the-Middle Attack (MITM)***

Note: Copyrights of this figure are reserved for original author

Alice

XA Pruck by YA public key

XA

8. K2 =YD2 mod 2

6.YD2

7

Bob

XB poinde kay JB public key 14. K1 =YDXB mod 9

2. YA/S. YB

XP2

3. Kgs YA modq Darth

XDI

XDI

7. K1 = YB mod q

XD2

princk kegs

[bey

YDI, YD2 public keys.

Bob & Alice share that they shore a secret.

But in fact kg is shared beth Alice & Darth K1 is shared beta

Bob & Darth

Figure 19.2 ***Man-in-the-Middle Attack (MITM)***

19.7 Activities (Problem Solving)

1. Given Prime number (C) = 23, Primitive root (D) = 5, Alice chooses her private key (E) = 6, Bob chooses his private key (F) = 15 . Find Public Keys and Secret key using Diffie-Hellman Key Exchange Algorithm.

19.8 Examples

19.8.1 Primitive Root

A number p is primitive root of q, if for i in 1 to q-1, p power of i mod q is less than q and unique.

For example 3 is a primitive root of 7.

33333

31

3

= 3 (mod 7)

32

9

N

2 (mod 7)

33

27

=

6 (mod 7)

34

81

=

4 (mod 7)

ვა

243

=

5 (mod 7)

ვნ

729

=

1 (mod 7)

Figure 19.3 ***Primitive Root Example***

19.8.2 Example on Diffie-Hellman Key Exchange Algorithm

Let's assume Alice and Bob want to establish a shared secret key using Diffie-Hellman. They agree on a prime number, "C," and a primitive root modulo "C," denoted as "D."

For this example, let's say:

Prime number (C) = 23

Primitive root (D) = 5

Now, Alice and Bob will independently choose their private keys and compute their public keys:

Private Key Selection:

Alice chooses her private key (E) = 6

Bob chooses his private key (F) = 15

Public Key Calculation:

Alice calculates her public key (A) using the formula A = D^E mod C: A = 5^6 mod 23 = 8 (Alice's public key)

Bob calculates his public key (B) using the formula B = D^F mod C: B = 5^15 mod 23 = 19 (Bob's public key)

Shared Secret Calculation:

Alice takes Bob's public key (B) and computes the shared secret key (s) using the formula S = B^E mod C.": s = 19^6 mod 23 = 2 (Alice's shared secret key)

Bob takes Alice's public key (A) and computes the shared secret key (s) using the formula S = A^F mod C.": s = 8^15 mod 23 = 2 (Bob's shared secret key)

Both Alice and Bob have reached the same shared secret key, which in this example is 2. Now they may continue communicating using this secret key they've both agreed upon, such as symmetric encryption or message authentication.

19.9 Table Numbering: NA

19.10 Figures with Captions

Figure 17.1 *Man-in-the-Middle Attack (MITM)*

Figure 17.2 *Man-in-the-Middle Attack (MITM)*

Figure 17.3 *Primitive Root Example*

19.11 Self Assessment Questions

1. Identify the purpose of Diffie-Hellman Key Exchange protocol :

   a) Encryption and decryption of data

   b) Digital signatures

   c) Secure key distribution

   d) Hashing algorithms

2. The mathematical concept that is used in Diffie-Hellman Key Exchange protocol is.

   a) Integer factorization

   b) Discrete logarithm

   c) Primality testing

   d) Modular arithmetic

3. The shared secret value which both entities agree In Diffie-Hellman Key Exchange:

   a) Public key

   b) Private key

   c) Symmetric key

   d) Hash value

4.Diffie-Hellman Key Exchange provides security against:

   a) Encryption algorithms

   b) Brute-force attacks

   c) Password cracking techniques

   d) Distributed denial-of-service (DDoS) attacks

5. Recognize the disadvantage of Diffie-Hellman Key Exchange?

   a) Efficient key exchange over insecure channels

   b) No need for prior communication or shared secrets

   c) Resistant to man-in-the-middle attacks

   d) Supports authentication of the communicating parties

6. Identify the cryptographic system used in Diffie-Hellman Key Exchange:

a) Symmetric encryption

b) Asymmetric encryption

c) Hash functions

d) Digital signatures

7. Attack possible on Diffie-Hellman Key Exchange is:

a) Replay attacks

b) MITM

c) Collision attacks

d) Timing attacks

8. Diffie-Hellman Key Exchange is a cryptographic protocol used to securely exchange ____________ over an insecure channel.

a) Plaintext

b) Keys

c) Ciphertext

d) None

9.The Diffie-Hellman Key Exchange algorithm is based on ____________ operations in modular arithmetic.

a)exponentiation.

b) arithmetic

c) logic

d) binary

10. The Diffie-Hellman Key Exchange algorithm involves the use of ____________ and ____________ parameters.

a) even, iterator

b) odd, iterator

c) prime, generator

d) prime, iterator

11. What is the Diffie-Hellman key exchange algorithm?

a) A method for securely exchanging cryptographic keys over insecure channels

b) A method for encrypting and decrypting data

c) A method for generating random numbers

d) A method for verifying the sender's identity

12. 12.What are the two main steps in the Diffie-Hellman key exchange algorithm?

a) Alice and Bob agree on a prime number and a base

b) Alice and Bob each choose a secret integer and compute a public key

c) Alice and Bob each send their public keys to the other party

d) Alice and Bob each compute the shared secret key

13.What is the shared secret key in the Diffie-Hellman key exchange algorithm?

a) The product of Alice's public key and Bob's public key

b) The sum of Alice's public key and Bob's public key

c) The difference of Alice's public key and Bob's public key

d) The modular exponentiation of Alice's public key and Bob's secret integer

14. What is the security of the Diffie-Hellman key exchange algorithm?

a) The security of the Diffie-Hellman key exchange algorithm depends on the difficulty of factoring large numbers

b) The security of the Diffie-Hellman key exchange algorithm depends on the difficulty of breaking the RSA algorithm

c) The security of the Diffie-Hellman key exchange algorithm depends on the difficulty of guessing Alice's secret integer

d) The security of the Diffie-Hellman key exchange algorithm depends on the difficulty of guessing Bob's secret integer.

15. Diffie-Hellman algorithm is widely known as

a) key exchange algorithm

b) key agreement algorithm

c) both a and b

d) None

16. What is the advantage of using the Diffie-Hellman key exchange algorithm over other key exchange algorithms?

a) The Diffie-Hellman key exchange algorithm is more secure than other key exchange algorithms

b) The Diffie-Hellman key exchange algorithm is faster than other key exchange algorithms

c) The Diffie-Hellman key exchange algorithm is easier to implement than other key exchange algorithms

d) The Diffie-Hellman key exchange algorithm is more scalable than other key exchange algorithms

17. What is the disadvantage of using the Diffie-Hellman key exchange algorithm?

a) The Diffie-Hellman key exchange algorithm is not very secure

b) The Diffie-Hellman key exchange algorithm is not very fast

c) The Diffie-Hellman key exchange algorithm is not very easy to implement

d) The Diffie-Hellman key exchange algorithm is not very scalable

18. What is the most common use of the Diffie-Hellman key exchange algorithm?

a) To encrypt and decrypt data

b) To verify the sender's identity

c) To generate random numbers

d) To exchange cryptographic keys

19. What is the future of the Diffie-Hellman key exchange algorithm?

a) The Diffie-Hellman key exchange algorithm will be replaced by a more secure algorithm

b) The Diffie-Hellman key exchange algorithm will be used alongside other algorithms for key exchange

c) The Diffie-Hellman key exchange algorithm will be used for digital signatures

d) The Diffie-Hellman key exchange algorithm will be used for encryption.

What is the minimum number of bits required for the prime number in the 20.Diffie-Hellman key exchange algorithm to be considered secure?

a) 1024 bits

b) 2048 bits

c) 4096 bits

d) 8192 bits

19.12 Summary

.

The Diffie-Hellman key exchange technique does not offer authentication or protection from active attacks. In order to guarantee the digital signature and or using the exchanged key within a secure communication protocol, are necessary to ensure the integrity and authenticity of the communication. To assure the security of the key exchange, large prime numbers are typically employed in real-world circumstances. Encryption, digital signatures, and secure communication.

19.13 Terminal Questions

1. Summarize Diffie-Hellman Algorithm.
2. Prove that a secret key is exchanged between source & destination.
3. Analyze attack on Diffie-Hellman Algorithm.
4. Consider a Diffie-Hellman scheme with a common prime and a primitive root 2 a. Show that 2 is a primitive root of 11. b. If user A has public key 9 , what is A’s private key ? c. If user B has public key 3 , what is the secret key shared with A?

19.14 Case studies: NA

19.15 Answer Key

Self-Assessment Questions

1. c) Secure key distribution
2. b) Discrete logarithm
3. c) Symmetric key
4. b) Brute-force attacks
5. d) Supports authentication of the communicating parties
6. b) Asymmetric encryption
7. b) MITM

8. b) Keys

9. a)exponentiation.

10. c) prime, generator

11. a) A method for securely exchanging cryptographic keys over insecure channels

12. b) Alice and Bob each choose a secret integer and compute a public key

13. d) The modular exponentiation of Alice's public key and Bob's secret Integer.

14. a) The security of the Diffie-Hellman key exchange algorithm depends on the difficulty of factoring large numbers

15. c) both a and b

16. a)The Diffie-Hellman key exchange algorithm is more secure than other key exchange algorithms.

17. c) The Diffie-Hellman key exchange algorithm is not very easy to implement

18. d) To exchange cryptographic keys

19. b) The Diffie-Hellman key exchange algorithm will be used alongside other algorithms for key exchange.

20. c) 4096 bits

Terminal Questions

1. The Diffie-Hellman key exchange algorithm is a protocol created to make it easier for two parties to establish a shared secret key via an unreliable channel. This algorithm was created by Whitfield Diffie and Martin Hellman in 1976 and is based on the idea of discrete logarithms. Its main benefit is that it makes it possible for two parties—typically referred to as Alice and Bob—to agree on a secret key without actually communicating it

- **Setup:**

Alice and Bob together must choose a prime number C a primitive root modulo often denoted as "D." These values are publicly known.

They also choose their own private keys: Alice selects "E," and Bob selects "F." These private keys are kept secret.

- **Key Generation:**

Alice computes her public key by calculating "A = D^E mod C" and sends it to Bob. Bob computes his public key by calculating "B = D^F mod C" and sends it to Alice.

- **Shared Secret Calculation:**

Alice computes the shared secret key using the formula "S = B^E mod C."

Bob computes the shared secret key using the formula "S = A^F mod C."

- **Shared Secret Exchange:**

After performing the calculations, both Alice and Bob have arrived at the same shared secret key, "s." This key can now be used for secure communication

2.

S = A^F mod C //Secret Key of Bob//

=(D^E mod C) ^F mod p // B is Public key of Bob//

=(D^E)^F mod C // by the rules of modular arithmetic//

= D^E^F mod C

= D^F^E mod C

= (D^F mod C) ^E mod p

= (D^F) ^E mod C

= B^E mod C // Secret Key of Alice//

Alice

XA Pruck by YA public key

XA

8. K2 =YD2 mod 2

6.YD2

7

Bob

XB poinde kay JB public key 14. K1 =YDXB mod 9

2. YA/S. YB

XP2

3. Kgs YA modq Darth

XDI

ノ

XDI

7. K1 = YB mod q

XD2

princk kegs

[bey

YDI, YD2 public keys.

Bob & Alice share that they shore a secret.

But in fact kg is shared beth Alice & Darth K1 is shared beta

Bob & Darth

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}

Alice transmits Y_A to Bob

Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates K2 = (Y_A) ^ X_{D2} mod q

Bob receives Y_{D1} and calculates K1=(Y_{D1}) ^ X_B mod q

Bob transmits Y_B to Alice

Darth intercepts Y_B and transmits Y_{D2} to Alice. Darth calculates K1= (Y_B) ^ X_{D1} mod q

Alice receives Y_{D2} and calculates K2 = (Y_{D2}) ^ X_A mod q

Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key k1 and Alice and Darth share secret key k2.

3. a. To show that 2 is a primitive root of 11, we need to verify that it generates all the elements in the range [1, 10] when raised to different powers modulo 11.

2^1 mod 11 = 2 2^2 mod 11 = 4 2^3 mod 11 = 8 2^4 mod 11 = 5 2^5 mod 11 = 10 2^6 mod 11 = 9 2^7 mod 11 = 7 2^8 mod 11 = 3 2^9 mod 11 = 6 2^10 mod 11 = 1

Since 2 generates all the numbers in the range [1, 10] modulo 11, we can conclude that 2 is a primitive root of 11.

b. If user A has a public key of 9, we need to find A's private key, denoted as "x," such that 2^x mod 11 = 9. To determine the value of x, we can calculate the discrete logarithm of 9 with base 2 modulo 11.

2^x mod 11 = 9

By trying different values of x, we find that x = 7 satisfies the equation:

2^7 mod 11 = 9

Therefore, A's private key is 7.

c. To calculate the secret key shared with A, we use user B's public key, denoted as "y," and raise it to A's private key modulo 11:

Secret key = (B's public key)^A's private key mod 11

Substituting the given values, we have:

Secret key = 3^7 mod 11

Calculating the value, we get:

Secret key = 2187 mod 11 Secret key = 10

Therefore, the secret key shared with A is 10.

19.16 Glossary

MITM- Man-in-the-Middle Attack

19.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm’s, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

19.18 Keywords

Diffie-Hellman, Elgamal, MITM

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 20

ELGAMAL CRYPTOSYSTEMS

20.1 Aim

To familiarize students with the basic concept of Diffie-Hellman Algorithm & Elgamal Algorithm.

20.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Diffie-Hellman Key Exchange Algorithm & Elgamal Cryptographic algorithm. It provides the necessary theoretical background and demonstrates how a secret key is exchanged between source and destinations. This session further allows students to apply Elgamal Cryptographic algorithm for various values of Plaintext.

20.3 Learning Outcomes

At the end of this session, students are expected to know

1. Apply Elgamal Algorithms to generate ciphertext.

20.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

20.5 Session Introduction

In this session, we will explore the fundamentals of public-key cryptography. The underlying principles of public-key cryptosystems are grounded in number theory, making use of mathematical functions rather than substitution and permutation techniques. Unlike symmetric encryption, which relies on a single key, public-key cryptography employs two distinct keys, giving rise to various implications for confidentiality, key distribution, and authentication. One prominent example of public-key cryptosystems that we will delve into is the Diffie-Hellman algorithm, along with the ElGamal algorithm.

20.6 Session Description

Elgamal Cryptosystems

- It is a public-key cryptographic algorithm.
- It was proposed by Taher ElGamal in 1985

Key Generation:

Select large prime number r and a primitive root modulo n

Select a private key, u, which is a random integer between 1 and r-2.

Find the public key, A, using A = n^u mod r.

Encryption:

Choose plaintext M

Choose a random integer, j, between 1 and r-2.

Calculate the shared secret, S, using S = A^j mod r.

Calculate the ciphertext pair (C1, C2) as follows:

C1 = n^j mod r

C2 = (M * S) mod r

Decryption:

To decrypt the ciphertext (C1, C2), the recipient uses their private key, a.

Calculate the shared secret, S, using S = C1^u mod r.

Calculate the inverse of S modulo r.

Retrieve the original message, M, by computing M = (C2 * inverse of S) mod p.

The discrete logarithm problem's computational complexity is what determines how secure the ElGamal algorithm is. Because this technique offers semantic security, a hacker cannot determine anything about the plaintext by examining the ciphertext.

ElGamal is an algorithm that can be used for digital signatures in addition to encryption. A variation of the encryption method is used for signing, and the recipient's public key is used to verify the signature during verification.

20.7 Activities (Problem Solving)

1. Given Prime number (C) = 23, Primitive root (D) = 5, Alice chooses her private key (E) = 6, Bob chooses his private key (F) = 15 . Find Public Keys and Secret key using Diffie-Hellman Key Exchange Algorithm.

20.8 Examples

<u>Example on Elgamal Cryptosystems</u>

Key Generation:

Select large prime number r and a primitive root modulo n

Select a private key, u, which is a random integer between 1 and r-2.

Find the public key, A, using A = n^u mod r.

Encryption:

Choose plaintext M

Choose a random integer, j, between 1 and r-2.

Calculate the shared secret, S, using S = A^j mod r.

Calculate the ciphertext pair (C1, C2) as follows:

C1 = n^j mod r

C2 = (M * S) mod r

Decryption:

To decrypt the ciphertext (C1, C2), the recipient uses their private key, a.

Calculate the shared secret, S, using S = C1^u mod r.

Calculate the inverse of S modulo r.

Retrieve the original message, M, by computing M = (C2 * inverse of S) mod p.

The discrete logarithm problem's computational complexity is what determines how secure the ElGamal algorithm is. Because this technique offers semantic security, a hacker cannot determine anything about the plaintext by examining the ciphertext.

Key Generation:

prime number r=23

primitive root n=7

The receiver (Bob) generates a key pair:

Private key (u) = 5

Public key (r, u, z) = (23, 7, 10) (where p is the prime number, g is the primitive root, and y = n^u mod r=7^5 mod 23=10

Encryption:

The sender (Alice) wants to encrypt a message for Bob.

Alice obtains Bob's public key (r, u, z) = (23, 7, 10)

Alice chooses a random value (k), let's say k = 6.

Alice performs the following calculations:

Find shared secret: s = z^k mod r = 10^6 mod 23 = 16

Plaintext is M=8

Ciphertext component 1: c1 = u^k mod r = 7^6 mod 23 = 19

Ciphertext component 2: c2 = (plaintext value * s) mod p = (8 * 16) mod 23 = 11

Ciphetext is (C1,C2)=(19, 11)

Decryption:

Bob receives the encrypted message: (19, 11).

Bob uses his private key (i = 5) to calculate the shared secret: s = (c1^i) mod r = (19^5) mod 23 = 16.

Plaintext = (c2 * (s^(-1))) mod p = (11 * (16^(-1))) mod 23 = 8

20.9 Table Numbering: NA

20.10 Figures with Captions: NA

20.11 Self Assessment Questions

2. The ElGamal cryptosystem is based on:

   a) Integer factorization problem

   b) Discrete logarithm problem

   c) Primality testing

   d) Elliptic curve cryptography

3. Which type of algorithm is ElGamal cryptosystem?

   a) Symmetric

   b) Asymmetric

   c) Hashing

   d) Stream

4. What is the other component apart from the encryption algorithm used in the ElGamal cryptosystem.

   a) Signature

   b) Decryption

   c) Key generation

   d) Hashing

5. In the ElGamal cryptosystem, the public key consists of:

   a) Only the encryption key

   b) Only the decryption key

   c) Both the encryption and decryption keys

   d) A hash value

6. The size of blocks used in ElGamal encryption algorithm are:

   a) Fixed-size blocks

   b) Variable-size blocks

   c) Single bits

   d) Hash values

7. ElGamal cryptosystem is considered secure under:

   a) RSA assumption

   b) Diffie-Hellman assumption

   c) Goldwasser-Micali assumption

   d) Decisional Diffie-Hellman assumption

8. The primary use of ElGamal cryptosystem is:

   a) Digital signatures

   b) Key exchange

   c) Data encryption

   d) Password hashing

9. The security of the ElGamal cryptosystem relies on the difficulty of:

   a) Integer factorization

   b) Primality testing

   c) Discrete logarithm

   d) Hash collision

10. ElGamal cryptosystem is vulnerable to:

   a) Side-channel attacks

   b) Brute-force attacks

   c) Collision attacks

   d) Differential cryptanalysis

10.Who designed ElGamal cryptosystem:

   a) Ronald Rivest, Adi Shamir, and Leonard Adleman

   b) Diffie and Hellman

   c) Taher Elgamal

   d) Whitfield Diffie

11. What are the two main steps in the Elgamal algorithm?

a) Key generation and encryption

b) Encryption and decryption

c) Key exchange and digital signature

d) Key generation and digital signature

12. What is the public key in the Elgamal algorithm?

a) A large prime number

b) A small integer

c) A random number

d) A pair of numbers

13. What is the private key in the Elgamal algorithm?

a) A large prime number

b) A small integer

c) A random number

d) A pair of numbers

14. What is the security of the Elgamal algorithm?

a) The security of the Elgamal algorithm depends on the difficulty of factoring large numbers

b) The security of the Elgamal algorithm depends on the difficulty of breaking the RSA algorithm

c) The security of the Elgamal algorithm depends on the difficulty of guessing the private key

d) The security of the Elgamal algorithm depends on the difficulty of guessing the public key.

15. What is the advantage of using the Elgamal algorithm over other asymmetric key encryption algorithms?

a) The Elgamal algorithm is more secure than other asymmetric key encryption algorithms

b) The Elgamal algorithm is faster than other asymmetric key encryption algorithms

c) The Elgamal algorithm is easier to implement than other asymmetric key encryption algorithms

d) The Elgamal algorithm is more scalable than other asymmetric key encryption algorithms.

16. What is the disadvantage of using the Elgamal algorithm over other asymmetric key encryption algorithms?

a) The Elgamal algorithm is not very secure

b) The Elgamal algorithm is not very fast

c) The Elgamal algorithm is not very easy to implement

d) The Elgamal algorithm is not very scalable

17. What is the most common use of the Elgamal algorithm?

a) To encrypt and decrypt data

b) To verify the sender's identity

c) To generate random numbers

d) To exchange cryptographic keys

18. What is the future of the Elgamal algorithm?

a) The Elgamal algorithm will be replaced by a more secure algorithm

b) The Elgamal algorithm will be used alongside other algorithms for encryption

c) The Elgamal algorithm will be used for digital signatures

d) The Elgamal algorithm will be used for key exchange

19. What is the minimum size of the modulus in the Elgamal algorithm to be considered secure?

a) 1024 bits

b) 2048 bits

c) 4096 bits

d) 8192 bits

20. What is the difference between the Elgamal algorithm and the RSA algorithm?

a) The Elgamal algorithm is asymmetric, while the RSA algorithm is symmetric

b) The Elgamal algorithm is slower, while the RSA algorithm is faster

c) The Elgamal algorithm is more secure, while the RSA algorithm is less secure

d) The Elgamal algorithm is used for encryption, while the RSA algorithm is used for key exchange

20.12 Summary

.The Diffie-Hellman key exchange technique does not offer authentication or protection from active attacks. In order to guarantee the digital signature and or using the exchanged key within a secure communication protocol, are necessary to ensure the integrity and authenticity of the communication. To assure the security of the key exchange, large prime numbers are typically employed in real-world circumstances. Encryption, digital signatures, and secure communication are all supported by the ElGamal algorithm in a variety of cryptographic applications. It's important to keep in mind that ElGamal is somewhat slower than some other public-key algorithms, including RSA.

20.13 Terminal Questions

1. Demonstrate Elgamal Algorithm.

2. consider a scenario where Bob wants to send a confidential message to Alice using the ElGamal cryptosystem. Alice's public key is (p, α, β), where p is a prime number, α is a primitive root modulo p, and β = α^a (mod p) is Alice's public key parameter. Bob wants to send the message M = 10 to Alice AND SECRET KEY K=7.

20.14 Case studies: NA

20.15 Answer Key

Assignment Questions

1. b) Discrete logarithm problem
2. b) Asymmetric
3. b) Decryption
4. a) Only the encryption key
5. b) Variable-size blocks
6. d) Decisional Diffie-Hellman assumption
7. c) Data encryption
8. c) Discrete logarithm
9. a) Side-channel attacks
10. c) Taher Elgamal
11. Key generation and encryption
12. d) A pair of numbers
13. b) A small integer
14. a) The security of the Elgamal algorithm depends on the difficulty of factoring large numbers.
15. a) The Elgamal algorithm is more secure than other asymmetric key encryption algorithms.
16. The Elgamal algorithm is not very easy to implement
17. a) To encrypt and decrypt data
18. b) The Elgamal algorithm will be used alongside other algorithms for Encryption.
19. b) 2048 bits

20. d) The Elgamal algorithm is used for encryption, while the RSA algorithm is used for key exchange.

Terminal Questions

1. Elgamal Cryptosystems

- It is a public-key cryptographic algorithm.
- It was proposed by Taher ElGamal in 1985

Key Generation:

Select large prime number r and a primitive root modulo n

Select a private key, u, which is a random integer between 1 and r-2.

Find the public key, A, using A = n^u mod r.

Encryption:

Choose plaintext M

Choose a random integer, j, between 1 and r-2.

Calculate the shared secret, S, using S = A^j mod r.

Calculate the ciphertext pair (C1, C2) as follows:

C1 = n^j mod r

C2 = (M * S) mod r

Decryption:

To decrypt the ciphertext (C1, C2), the recipient uses their private key, a.

Calculate the shared secret, S, using S = C1^u mod r.

Calculate the inverse of S modulo r.

Retrieve the original message, M, by computing M = (C2 * inverse of S) mod p.

The discrete logarithm problem's computational complexity is what determines how secure the ElGamal algorithm is. Because this technique offers semantic security, a hacker cannot determine anything about the plaintext by examining the ciphertext.

ElGamal is an algorithm that can be used for digital signatures in addition to encryption. A variation of the encryption method is used for signing, and the recipient's public key is used to verify the signature during verification.

2. K = α^k (mod p) = 3^7 (mod 17) = 13

S = β^k (mod p) = β^7 (mod 17) = (α^a)^k (mod p) = (3^a)^7 (mod 17) = (3^4)^7 (mod 17) = 13^7 (mod 17) = 4^7 (mod 17) = 16

$C1 = \alpha^k \ (\text{mod } p) = 3^7 \ (\text{mod } 17) = 13$ $C2 = (M * S) \ (\text{mod } p) = (10 * 16) \ (\text{mod } 17) = 160 \ (\text{mod } 17) = 10$

Bob sends the ciphertext (C1, C2) = (13, 10) to Alice.

$S' = C1^a \ (\text{mod } p) = 13^a \ (\text{mod } 17) = (3^7)^a \ (\text{mod } 17) = (3^a)^7 \ (\text{mod } 17) = \beta^7 \ (\text{mod } 17) = S$

$S'^{(-1)} \ (\text{mod } p) = S^{(-1)} \ (\text{mod } p) = 16^{(-1)} \ (\text{mod } 17) = 13 \ (\text{mod } 17) = 13$

$M' = C2 * S'^{(-1)} \ (\text{mod } p) = 10 * 13 \ (\text{mod } 17) = 130 \ (\text{mod } 17) = 5$

The original message that Alice receives is 5.

Therefore, the original message sent by Bob to Alice using the ElGamal cryptosystem is 5.

20.16 Glossary

MITM- Man-in-the-Middle Attack

20.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm's, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

20.18 Keywords

Diffie-Hellman, Elgamal, MITM

CRYPTANALYSIS & CYBER DEFENSE

21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 21

ELLIPTIC CURVE ARITHMETIC

21.1 Aim

To familiarize students with the basic concept and equations of Elliptic Curve Arithmetic

21.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Elliptic Curves. It provides the necessary theoretical background and summarizes properties od Abelian Group. This session further allows students to apply Elliptic curve arithmetic over prime curves and binary curves.

21.3 Learning Outcomes

At the end of this session, students are expected to know

1. Summarizes properties of Abelian Group.
2. Differentiates Prime Curves and Binary Curves
3. Apply Elliptic Curve Arithmetic over Prime Curves

21.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

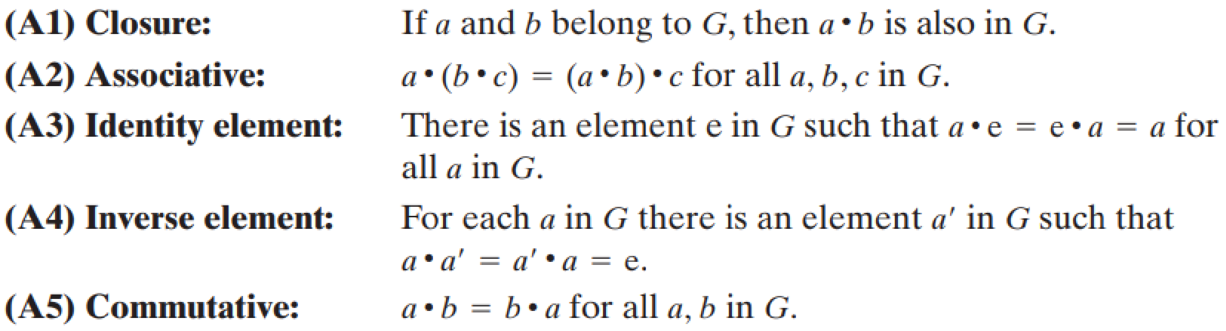
21.5 Session Introduction

This Session provides an overview of Elliptic curves. A number of elliptic curve cryptography (ECC) techniques, such as key exchange, encryption, and digital signature, can be created using elliptic curve arithmetic are discussed. The equation's variables and coefficients are components of a finite field.

21.6 Session Description

21.6.1 Abelian Group

Abelian group are used in design and analysis of cryptographic protocols. It is a mathematical structure consisting of a set of elements and an operation (typically denoted as '+') that satisfies the group axioms.An Abelian group is commutative, which means that the order in which the elements are combined using the group operation does not affect the result.



(A1) Closure: If a and b belong to G, then $a \bullet b$ is also in G.

(A2) Associative: $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \bullet \mathrm{e} = \mathrm{e} \bullet a = a$ for all a in G.

(A4) Inverse element: For each a in G there is an element a' in G such that $a \bullet a' = a' \bullet a = \mathrm{e}$.

(A5) Commutative: $a \bullet b = b \bullet a$ for all a, b in G.

Figure 21.1 Properties of Abelian Group

21.6.2 Elliptic Curve Arithmetic

Elliptic Curves are 2 types, (i) prime curves and (ii) binary curves.

For a prime curve over Zp we use cubic equation in which variables & coefficients all takes values from 0 to p-1 in which calculations are performed over modulo p. Best for s/w applications.

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

For a binary curve over GF(2^m), the variables & coefficients all take on values in GF(2^m) and calculations are performed over GF(2m). Best for h/w applications.

$$y^2 + xy = x^3 + ax^2 + b$$

21.6.3 Elliptic Curve Arithmetic- Prime Curves (Zp)

- **Curve Equation:**

A prime curve is defined by an equation in the form y^2 = x^3 + ax + b mod p, where a and b are coefficients, and p is a prime number. A+O=A

- **Negative of a Point:** If A = (x_1, y_1) then –A= (x_1, -y_1))= (x_1, -$y_{1\ \mathrm{mod}}$ p)
- **Point Addition:**

Given two points A = (x_1, y_1) and B = (x_2, y_2) on the curve, the sum C = A + B= (x_3, y_3) is computed and A not equal to B

$x_{3\,=\,(}\ \lambda^2 - x_1 - y_2)$mod p

$y_{3\,=}\ (\lambda(x_1 - x_3) - y_1)$ mod p

λ= (y_2- y_1)/ (x_2- x_1) mod p if A equal to B

λ= ($3x_1^2$+a)/ ($2y_1$) mod p if A not equal to B

- **Point Multiplication:** It is repeated addition. 3A=A+A+A

21.7 Activities (Problem Solving)

Consider an elliptic curve E defined over the prime field F_19 with the equation y^2 = x^3 + 3x + 10. The base point G on the curve is (8, 4). Find the result of the following computation: 5G.

21.8 Examples

Elliptic Curve Arithmetic- Prime Curves (Zp)

Consider the elliptic curve defined over *$Z_{23)}$* with the equation y^2 = x^3 + 5x + 7

Curve Equation: y^2 = x^3 + 5x + 7 (mod 23)

Point Addition: Let's take two points, A(3, 6) and B(17, 19), on the curve.

Case 1: A and B are distinct points. slope λ = (y_2- y_1)/ (x_2- x_1) mod p= (19 - 6)/(17 - 3) = 13/14 ≡ 13 * 14^-1 (mod 23)

Now, we find the multiplicative inverse of 14 modulo 23: 14^-1 ≡ 19 (mod 23)

Therefore, the slope λ is 13 * 19 ≡ 6 (mod 23).

Next, we calculate the sum of A and B: x_3 = λ ^2 - x_1 - x_2 ≡ 6^2 - 3 - 17 ≡ 17 (mod 23)

y_3 = λ * (x_1 - x_3) - y_1 ≡ 6 * (3 - 17) - 6 ≡ 10 (mod 23)

Thus, the sum of A and B is C(17, 10).

Case 2: A and B are the same point. to the curve at point A. slope λ = (3 * 3 + 5)/(2 * 6) ≡ 16/12 ≡ 16 * 12^-1 (mod 23)

The multiplicative inverse of 12 modulo 23 is: 12^-1 ≡ 2 (mod 23)

Hence, the slope λ is 16 * 2 ≡ 9 (mod 23).

The sum of A and A (point doubling) is then calculated as: x_3 = λ ^2 - 2x_1 ≡ 9^2 - 2 * 3 ≡ 4 (mod 23) y_3 = slope * (x_1 - x_3) - y_1 ≡ 9 * (3 - 4) - 6 ≡ 3 (mod 23)

Therefore, the sum of A and A is C(4, 3).

Scalar Multiplication: Let's perform scalar multiplication on a point A(3, 6) with a scalar value of 5.

Start with A = (3, 6).

Double the point: 2A = A+ A= C(4, 3).

Double the point: 4A = 2A + 2A = C(4, 3) + C(4, 3) = D(18, 11).

Double the point: 16A = 8A + 8A = C(16, 0) + C(16, 0) = O (point at infinity).

21.9 Table Numbering: NA

21.10 Figures with Captions

Figure 21.1 Properties of Abelian Group

21.11 Self Assessment Questions

1 Which of the following is a property of an Abelian group?

a) Closure under addition

b) Closure under multiplication

c) Closure under both addition and multiplication

d) Closure under division

2. An Abelian group is a group in which:

a) The identity element is unique

b) Every element has an inverse

c) The group operation is commutative

d) All of the above

3. Which of the following is an example of an Abelian group?

a) The set of integers with addition as the group operation

b) The set of real numbers with multiplication as the group operation

c) The set of rational numbers with addition as the group operation

d) The set of positive integers with subtraction as the group operation

4. In an Abelian group, the operation satisfies the property of:

a) Associativity

b) Distributivity

c) Commutativity

d) Identity

5. Which of the following is not true for an Abelian group?

a) Every element has a unique inverse

b) The group operation is associative

c) The group operation is commutative

d) The group operation is distributive

6. Which of the following is an example of a non-Abelian group?

a) The set of square matrices with addition as the group operation

b) The set of positive integers with multiplication as the group operation

c) The set of rational numbers with addition as the group operation

d) The set of integers with subtraction as the group operation

7. An Abelian group is also known as a:

a) Cyclic group

b) Symmetric group

c) Non-Abelian group

d) Commutative group

8. In an Abelian group, the identity element is denoted by:

a) 0

b) 1

c) e

d) I

9. Which property is not required for an Abelian group?

a) Inverse property

b) Closure property

c) Associative property

d) Distributive property

10. Which mathematical structure is a generalization of an Abelian group?

a) Vector space

b) Field

c) Ring

d) Module

11. What is the general equation for elliptic curve systems?

a) y3+b_1 xy+b_2 y=x33+a_1 x2+a_2 x+a_3

b) y3+b_1 x+b_2 y=x2+a_1 x2+a_2 x+a_3

c) y2+b_1 xy+b_2 y=x3+a_1 x2+a_2

d) y2+b_1 xy+b_2 y=x3+a_1 x2+a_2 x+a_3

12. In Singular elliptic curve, the equation x^3+ax+b=0 does ____ roots.

a) does not have three distinct

b) has three distinct

c) has three unique

d) has three distinct unique

13. In the elliptic curve group defined by y2= x3- 17x + 16 over real numbers, what is 2P if P = (4, 3.464)?

a) (12.022, -39.362)

b) (32.022, 42.249)

c) (11.694, -43.723)

d) (43.022, 39.362)

14.What is the general equation for elliptic curve systems?

a)y^2 = x^3 + ax + b

b)y^2 = x^3 - ax + b

c)y^2 = x^3 + b

d)y^2 = x^3 – b

15.“Elliptic curve cryptography follows the associative property.”

a)True

b)False

c)It depends on the elliptic curve

d)It depends on the finite field

16.Which of the following is not a property of elliptic curve cryptography?

a)It is based on the algebraic structure of elliptic curves over finite fields.

b)It allows smaller keys compared to non-EC cryptography to provide equivalent security.

c)It is more secure than RSA cryptography.

d)It is faster than RSA cryptography.

17.What is the inverse of point P = (x1, y1) in ECC?

a)(x1, -y1)

b)(-x1, y1)

c)(x1, y1)

d)(-x1, -y1)

18.What is the order of an elliptic curve point P?

a)The number of times P can be added to itself to get the point (0, 0).

b)The number of times P can be doubled to get the point (0, 0).

c)The number of times P can be added to itself to get the point (1, 0).

d)The number of times P can be doubled to get the point (1, 0).

19. What is the security of elliptic curve cryptography?

a) ECC is considered to be as secure as RSA, if not more secure.

b) ECC is not as secure as RSA.

c) ECC is not as widely used as RSA.

d) ECC is not as efficient as RSA.

20.What are the advantages of elliptic curve cryptography?

a) ECC allows smaller keys compared to RSA to provide equivalent security.

b) ECC is faster than RSA.

c) ECC is more efficient in terms of memory usage.

d) All of the above.

21.12 Summary

Choosing the appropriate Abelian groups with well-defined security properties is crucial in cryptographic protocol design. The properties and computational complexity of the underlying Abelian group have a significant impact on the security and efficiency of the cryptographic schemes built on them.

Elliptic curve arithmetic plays a vital role in ensuring the security and efficiency of elliptic curve cryptography. By utilizing the unique properties of elliptic curves, cryptographic protocols can achieve robust security with smaller key sizes compared to other schemes.

The Elliptic Curve Diffie-Hellman (ECDH) algorithm offers a secure method for two parties to establish a shared secret key over an insecure channel without directly exchanging the secret. ECDH finds extensive application in scenarios where secure key exchange is essential, such as secure communication protocols and establishing secure connections in TLS/SSL.

21.13 Terminal Questions

1. Is (4, 7) a point on the elliptic curve over real numbers?

2. For Z_{11} (1,6) , consider the point G= (2,7) . Compute the value 2G

3. What are the negatives of the following elliptic curve points over Z_{17}? P = (5, 8); Q = (3, 0); R = (0, 6).

4. Illustrate Elliptic curve arithmetic over prime curves Z_p.

21.14 Answer Key

Self-Assessment Questions

1. a) Closure under addition

2. d) All of the above

3. a) The set of integers with addition as the group operation

4. c) Commutativity

5. d) The group operation is distributive

6. a) The set of square matrices with addition as the group operation

7. d) Commutative group

8. c) e

9. d) Distributive property

10. c) Ring

11. d) y2+b_1 xy+b_2 y=x3+a_1 x2+a_2 x+a_3

12. a) does not have three distinct

13. a) (12.022, -39.362)

14. a)y^2 = x^3 + ax + b

15. a)True

16. c)It is more secure than RSA cryptography.

17. b)(-x1, y1)

18. a)The number of times P can be added to itself to get the point (0, 0).

19. a) ECC is considered to be as secure as RSA, if not more secure

20. d) All of the above.

Terminal Questions

1. To determine if the point (4, 7) lies on an elliptic curve over real numbers, we need to substitute the values of x and y into the equation of the curve and check if it holds true.

Let's assume the equation of the elliptic curve is y^2 = x^3 + ax + b, where a and b are constants.

In this case, we have y^2 = x^3 + ax + b, and we need to check if (4, 7) satisfies this equation.

Substituting x = 4 and y = 7 into the equation, we get:

7^2 = 4^3 + a * 4 + b

49 = 64 + 4a + b

Since 49 is not equal to 68 + 4a + b, (4, 7) does not lie on the elliptic curve over real numbers defined by the given equation.

Therefore, (4, 7) is not a point on the elliptic curve over real numbers.

2. Given the elliptic curve over Z11: $y^2 \equiv x^3 + ax + b \pmod{11}$, and the point G = (2, 7). To calculate 2G, we'll perform the following steps:
Compute the slope (m) of the tangent line passing through G.

$m = (3 * x_1^2 + a) * (2 * y_1)^{-1} \pmod{11} = (3 * 2^2 + a) * (2 * 7)^{-1} \pmod{11} = (12 + a) * (14)^{-1} \pmod{11} = (a + 1) * 8 \pmod{11}$

Compute the x-coordinate of the point 2G.

$x_2 = (m^2 - 2 * x_1) \pmod{11} = ((a + 1)^2 * 8^2 - 2 * 2) \pmod{11}$

Compute the y-coordinate of the point 2G.

$y_2 = (m * (x_1 - x_2) - y_1) \pmod{11} = (m * (2 - x_2) - 7) \pmod{11}$

Now, substitute the values of x_1 and y_1 into the above equations to find x_2 and y_2.

$x_2 = ((a + 1)^2 * 8^2 - 2 * 2) \pmod{11}$

$y_2 = ((a + 1) * 8 * (2 - x_2) - 7) \pmod{11}$

Please provide the value of 'a' in the equation of the elliptic curve, $y^2 \equiv x^3 + ax + b \pmod{11}$, to compute 2G accurately.

3. To find the negatives of the given elliptic curve points over Z17, we need to negate the y-coordinate of each point while keeping the x-coordinate the same.
Given the points in Z17: P = (5, 8), Q = (3, 0), and R = (0, 6).
The negatives of these points can be calculated as follows:
Negative of P: P' = (x, -y) mod 17 = (5, -8) mod 17 = (5, 9)
Negative of Q: Q' = (x, -y) mod 17 = (3, -0) mod 17 = (3, 0)
Negative of R: R' = (x, -y) mod 17 = (0, -6) mod 17 = (0, 11)
Therefore, the negatives of the given elliptic curve points over Z17 are: P' = (5, 9) Q' = (3, 0) R' = (0, 11)
4. Consider the elliptic curve defined over Z23) with the equation $y^2 = x^3 + 5x + 7$
Curve Equation: $y^2 = x^3 + 5x + 7 \pmod{23}$

Point Addition: Let's take two points, A(3, 6) and B(17, 19), on the curve.

Case 1: A and B are distinct points. slope λ = (y2- y1)/ (x2- x1) mod p= (19 - 6)/(17 - 3) = 13/14 ≡ 13 * 14^-1 (mod 23)

Now, we find the multiplicative inverse of 14 modulo 23: 14^-1 ≡ 19 (mod 23)

Therefore, the slope λ is 13 * 19 ≡ 6 (mod 23).

Next, we calculate the sum of A and B: x3 = λ ^2 - x1 - x2 ≡ 6^2 - 3 - 17 ≡ 17 (mod 23)

y3 = λ * (x1 - x3) - y1 ≡ 6 * (3 - 17) - 6 ≡ 10 (mod 23)

Thus, the sum of A and B is C(17, 10).

Case 2: A and B are the same point. to the curve at point A. slope λ = (3 * 3 + 5)/(2 * 6) ≡ 16/12 ≡ 16 * 12^-1 (mod 23)

The multiplicative inverse of 12 modulo 23 is: 12^-1 ≡ 2 (mod 23)

Hence, the slope λ is 16 * 2 ≡ 9 (mod 23).

The sum of A and A (point doubling) is then calculated as: x3 = λ ^2 - 2x1 ≡ 9^2 - 2 * 3 ≡ 4 (mod 23) y3 = slope * (x1 - x3) - y1 ≡ 9 * (3 - 4) - 6 ≡ 3 (mod 23)

Therefore, the sum of A and A is C(4, 3).

Scalar Multiplication: Let's perform scalar multiplication on a point A(3, 6) with a scalar value of 5.

Start with A = (3, 6).

Double the point: 2A = A+ A= C(4, 3).

Double the point: 4A = 2A + 2A = C(4, 3) + C(4, 3) = D(18, 11).

Double the point: 16A = 8A + 8A = C(16, 0) + C(16, 0) = O (point at infinity).

4. **Curve Equation:**

A prime curve is defined by an equation in the form y^2 = x^3 + ax + b mod p, where a and b are coefficients, and p is a prime number. A+O=A

5. **Negative of a Point:** If A = (x_1, y_1) then –A= $(x_1, -y_1)$)= $(x_1, -y_{1\ mod}$ p)

6. **Point Addition:**

Given two points A = (x_1, y_1) and B = (x_2, y_2) on the curve, the sum C = A + B= (x_3, y_3) is computed and A not equal to B

$x_3 = (\lambda^2 - x_1 - y_2)$mod p

$y_3 = (\lambda(x_1 - x_3) - y_1)$ mod p λ= $(y_2 - y_1)/(x_2 - x_1)$ mod p if A equal to B

λ= $(3x_1^2+a)/(2y_1)$ mod p if A not equal to B

7.Point Multiplication: It is repeated addition. 3A=A+A+A

21.15 Case Studies: NA

21.16 Glossary

ECC – Elliptic Curve Cryptography

ECDH - Elliptic Curve Diffie-Hellman Key Exchange

21.17 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm's, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

21.17 b Keywords

Elliptic Curve Arithmetic, Elliptic Curve Cryptography

CRYPTANALYSIS & CYBER DEFENSE
21CS3041RA

Course Description

This course provides an introduction to the core principles of cryptography and its relevance in the field of network security. Students will gain a comprehensive understanding of cryptographic methods used to ensure secure communication in potentially insecure environments. Topics covered include techniques for verifying message source authenticity, ensuring message integrity during transmission across unsecured channels, and establishing unique message origin identification. The course also addresses cryptanalysis attacks on cryptographic techniques, as well as various attack models.

SESSION: 22
ELLIPTIC CURVE ARITHMETIC & CRYPTOGRAPHY

22.1 Aim

To familiarize students with the basic concept and equations of Elliptic Curve Arithmetic & cryptography.

22.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Elliptic Curves. It provides the necessary theoretical background and summarizes properties od Abelian Group. This session further allows students to apply Elliptic curve arithmetic over prime curves and binary curves. This session also demonstrates Elliptic curve cryptography.

22.3 Learning Outcomes

At the end of this session, students are expected to know

1. Apply Elliptic Curve Arithmetic Binary Curves
2. Illustrates Elliptic Curve Diffie-Hellman Key Exchange Algorithm.

22.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

22.5 Session Introduction

This Session provides an overview of Elliptic curves. A number of elliptic curve cryptography (ECC) techniques, such as key exchange, encryption, and digital signature, can be created using elliptic curve arithmetic are discussed. The usage of an elliptic curve equation over a finite field Zp and GF(2^m) is required for elliptic curve arithmetic in the context of ECC. The equation's variables and coefficients are components of a finite field.

22.6 Session Description

<u>22.6.1 Elliptic Curve Arithmetic- Binary Curves GF(2^m)</u>

- **Curve Equation:**

A binary curve is defined by an equation in the form y^2 + xy = x^3 + ax^2 + b, where a and b are coefficients, and the arithmetic is performed over a finite field of characteristic 2. The equation represents points (x, y) on the curve that satisfy the equation, along with a point at infinity, denoted as O.

- **Negative of a Point:** If A = (x_1, y_1) then –A= (x_1, $x_{1+}y_{1\ mod}$ p)
- **Point Addition:**

Given two points A = (x_1, y_1) and B = (x_2, y_2) on the curve, the sum C = A + B= (x_3, y_3) is computed.

$x_{3\,=}\ \lambda^2 + \lambda\ _+\ x_1 + x_2 + a$

$y_{3\,=}\ (\lambda(x_1+x_3)+x_3+ y_1$

$\lambda = (y_2+y_1)/\ (x_2+x_1)$ mod p

- **Point Multiplication:** It is repeated addition. 3A=A+A+A

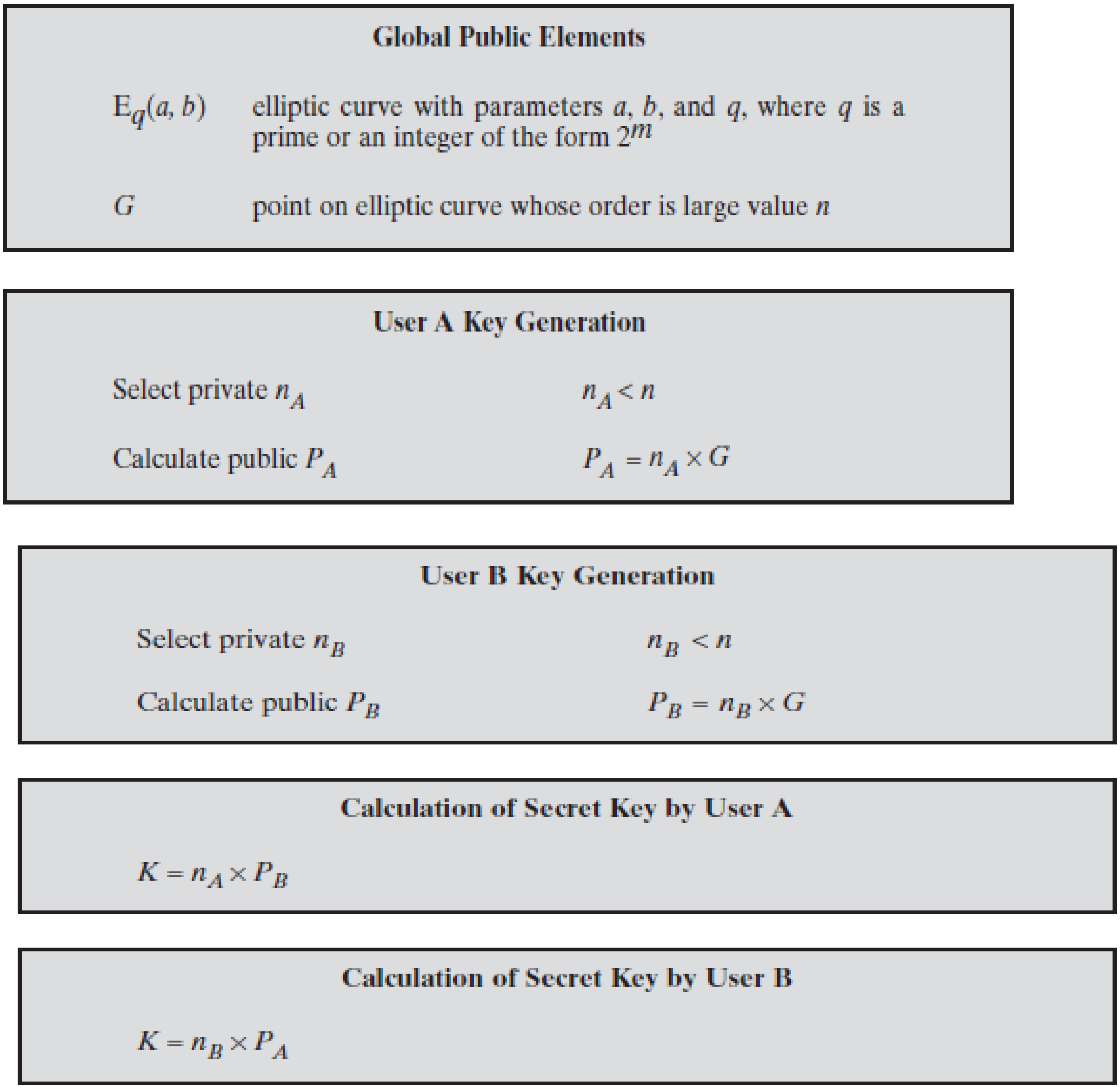
$x_{3\,=}\ \lambda^2 + \lambda + a$

$y_{3\,=}\ x_1^2 + (\lambda + x_3)$

$\lambda = x_1 + y_{1/}\ x_1$

<u>22.6.2 ECC Diffie-Hellman Key Exchange</u>

The Diffie-Hellman key exchange algorithm can be adapted to use elliptic curve cryptography (ECC) instead of traditional modular arithmetic. This variant is called Elliptic Curve Diffie-Hellman (ECDH) key exchange. Here's how ECDH works::



Global Public Elements

$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation

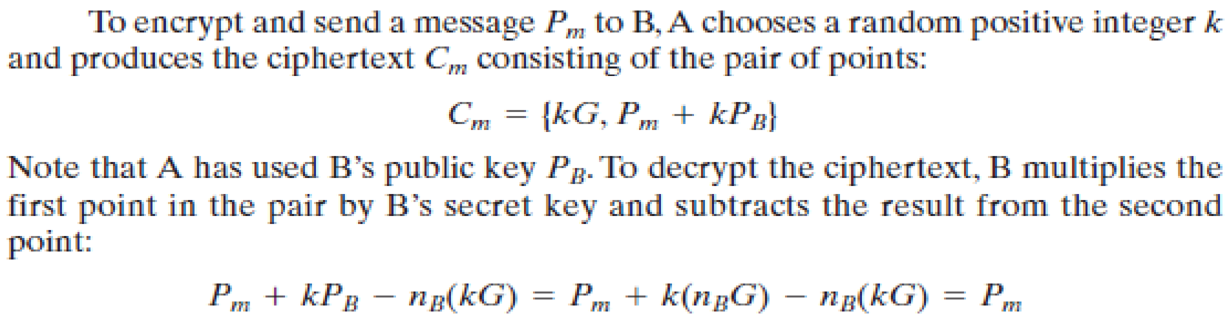
Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$



To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

Figure 20.1 ECC Diffie-Hellman Key Exchange Algorithm

Note: Copyrights of this figure are reserved for original author

22.7 Activities (Problem Solving)

Consider an elliptic curve defined over a binary field (GF(2^m)) given by the equation:

E: y^2 + xy = x^3 + ax^2 + b

where a and b are coefficients of the curve. Let's say we have the following parameters:

a = 1 (binary representation: 01) b = 0 (binary representation: 00) Field size: GF(2^4) (i.e., m = 4)

Now, let's perform elliptic curve arithmetic operations on this binary curve.

Point Addition: Given two points on the curve: P = (x1, y1) = (0110, 0011) Q = (x2, y2) = (1101, 0101)

22.8 Examples

Elliptic Curve Arithmetic- Binary Curves GF(2^m)

Consider the binary elliptic curve defined by the equation y^2 + xy = x^3 + x^2 + 1 over the finite field GF(2^8) using irreducible polynomial m(x) = x^8 + x^4 + x^3 + x + 1.

Curve Equation: y^2 + xy = x^3 + x^2 + 1 (mod m(x))

Point Addition: Let's take two points, A(1101, 0100) and A(1011, 0111), on the curve.

Case 1: A and B are distinct points. We calculate the slope of the line passing through A and B: slope λ = (y_2 + y_1) / (x_2 + x_1) = (0111 + 0100) / (1011 + 1101) = 1011 / 0110 (mod 2) Now, we perform polynomial division in GF(2^8) to find the slope: 1011 / 0110 = 1101 (quotient) with a remainder of 1001 (mod m(x))

Therefore, the slope λ is 1101 (mod m(x)).

Next, we calculate the sum of A and B: x_3 = λ ^2 + λ + x1 + x2 = 1101^2 + 1101 + 1101 + 1011 = 0001 (mod m(x)) y_3 = λ * (x_1 + x_3) + y1 = 1101 * (1101 + 0001) + 0100 = 0100 (mod m(x))

Thus, the sum of A and B is C(0001, 0100).

Case 2: A and B are the same point. In this case, we need to find the tangent line to the curve at point A. slope λ = (3 * x1^2 + 2 * x1 + 1) / (2 * y1 + x1) = (3 * 1101^2 + 2 * 1101 + 1) / (2 * 0100 + 1101) (mod 2)

Calculating the numerator: 3 * 1101^2 + 2 * 1101 + 1 = 1000 (mod m(x))

Calculating the denominator: 2 * 0100 + 1101 = 1000 (mod m(x))

Therefore, the slope λ is 1000 (mod m(x)).

The sum of A and A (point doubling) is then calculated as: x_3 = λ ^2 + slope + x_1 = 1000^2 + 1000 + 1101 = 1100 (mod m(x)) y_3 = λ * (x_1 + x_3) + y_1 = 1000 * (1101 + 1100) + 0100 = 0111 (mod m(x))

Therefore, the sum of A and B is C(1100, 0111).

Scalar Multiplication: Let's perform scalar multiplication on a point A(1101, 0100) with a scalar value of 5.

Start with A = (1101, 0100).

Double the point: 2A = A+ A = R(1100, 0111).

Double the point: 4P = 2A + 2A

22.7 Table Numbering: NA

22.8 Figures with Captions

Figure 22.1 ECC Diffie-Hellman Key Exchange Algorithm

22.9 Self Assessment Questions

1. In elliptic curve arithmetic over binary fields, the coefficients of the curve equation are typically represented using:

a) Binary digits

b) Decimal digits

c) Hexadecimal digits

d) Real numbers

2. The addition operation in binary curve arithmetic involves adding the coordinates of two points and finding the result modulo:

a) 2

b) 3

c) 4

d) The field size

3. Which of the following formulas is used for point doubling in binary curve arithmetic?

a) s = (y2 + y1) / (x2 + x1)

b) x3 = s^2 + s + x1 + x2 + a

c) y3 = s(x1 + x3) + x3 + y1

d) None of the above

4. The binary curve arithmetic allows for faster computations compared to prime curve arithmetic because:

a) Binary arithmetic is simpler

b) Binary curves have more efficient algorithms

c) Binary curves have a smaller field size

d) Binary curves have fewer points

5. The binary curve arithmetic is commonly used in applications that require:

a) High security

b) Fast computations

c) Large field sizes

d) Low memory usage

6. Elliptic curve cryptography is based on the algebraic structure of:

a) Prime numbers

b) Finite fields

c) Binary numbers

d) Quadratic equations

7. The security of elliptic curve cryptography is based on the difficulty of solving the:

a) Elliptic curve discrete logarithm problem

b) Elliptic curve factorization problem

c) Elliptic curve prime factor problem

d) Elliptic curve modular inverse problem

8. In elliptic curve cryptography, the private key is a randomly chosen:

a) Prime number

b) Elliptic curve point

c) Bit string

d) Encryption key

9. The public key in elliptic curve cryptography is derived from the:

a) Private key

b) Hash function

c) Random number generator

d) Diffie-Hellman algorithm

10. The main advantage of elliptic curve cryptography compared to traditional public-key cryptography is:

a) Smaller key sizes for equivalent security

b) Faster encryption and decryption algorithms

c) Stronger resistance against attacks

d) Simpler key management and distribution

11. What are binary curves?

a) Elliptic curves over finite fields of the form GF(2^m).

b) Elliptic curves over finite fields of the form GF(p).

c) Elliptic curves over real numbers.

d) Elliptic curves over complex numbers.

12) What are the advantages of using binary curves in cryptography?

a) They are more efficient in terms of computation and memory usage.

b) They are more secure than other types of elliptic curves.

c) They are easier to implement in hardware.

d) All of the above.

13) What is the difference between binary curves and prime curves?

a) Binary curves are defined over finite fields of the form GF(2^m), while prime curves are defined over finite fields of the form GF(p).

b) Binary curves are more efficient in terms of computation and memory usage, while prime curves are more secure.

c) Binary curves are easier to implement in hardware, while prime curves are easier to implement in software.

d) All of the above.

14) What is the security of binary curves?

a) Binary curves are considered to be as secure as prime curves, if not more secure.

b) Binary curves are not as secure as prime curves.

c) Binary curves are not as widely used as prime curves.

d) Binary curves are not as efficient as prime curves.

15) What are the applications of binary curves in cryptography?

a) They can be used for digital signatures, key exchange, and encryption.

b) They can be used for secure communication over the internet.

c) They can be used for storing sensitive data.

d) All of the above.

16) Which of the following is a key advantage of ECC Diffie-Hellman Key Exchange over the original Diffie-Hellman Key Exchange?

a) It uses smaller key sizes to achieve the same level of security.

b) It is more resistant to attack.

c) It is faster.

d) All of the above.

Answer: (a)

17) Which of the following is NOT a part of the ECC Diffie-Hellman Key Exchange protocol?

a) Alice and Bob generate their own elliptic curve public-private key pairs.

b) Alice sends her public key to Bob.

c) Bob calculates a shared secret using his private key and Alice's public key.

d) Bob sends his public key to Alice.

18) The key size of ECC Diffie-Hellman Key Exchange is typically:

a) 128 bits.

b) 256 bits.

c) 512 bits.

d) 1024 bits.

19) ECC Diffie-Hellman Key Exchange is used in which of the following protocols?

a) TLS.

b) SSH.

c) IKEv2.

d) All of the above.

20) Which of the following is a potential drawback of ECC Diffie-Hellman Key Exchange?

a) It is not as well-known as the original Diffie-Hellman Key Exchange.

b) It requires more specialized hardware to implement.

c) It is not as secure as other key exchange protocols.

d) It is not as widely supported by applications.

22.10 Summary

It's important to choose appropriate Abelian groups with well-defined security properties when designing cryptographic protocols. The properties and computational complexity of the underlying Abelian group can significantly impact the security and efficiency of the cryptographic schemes built upon them.

The properties and computations associated with elliptic curve arithmetic provide a solid foundation for the security and efficiency of elliptic curve cryptography. By leveraging the unique properties of elliptic curves, cryptographic protocols can achieve strong security with comparatively smaller key sizes.

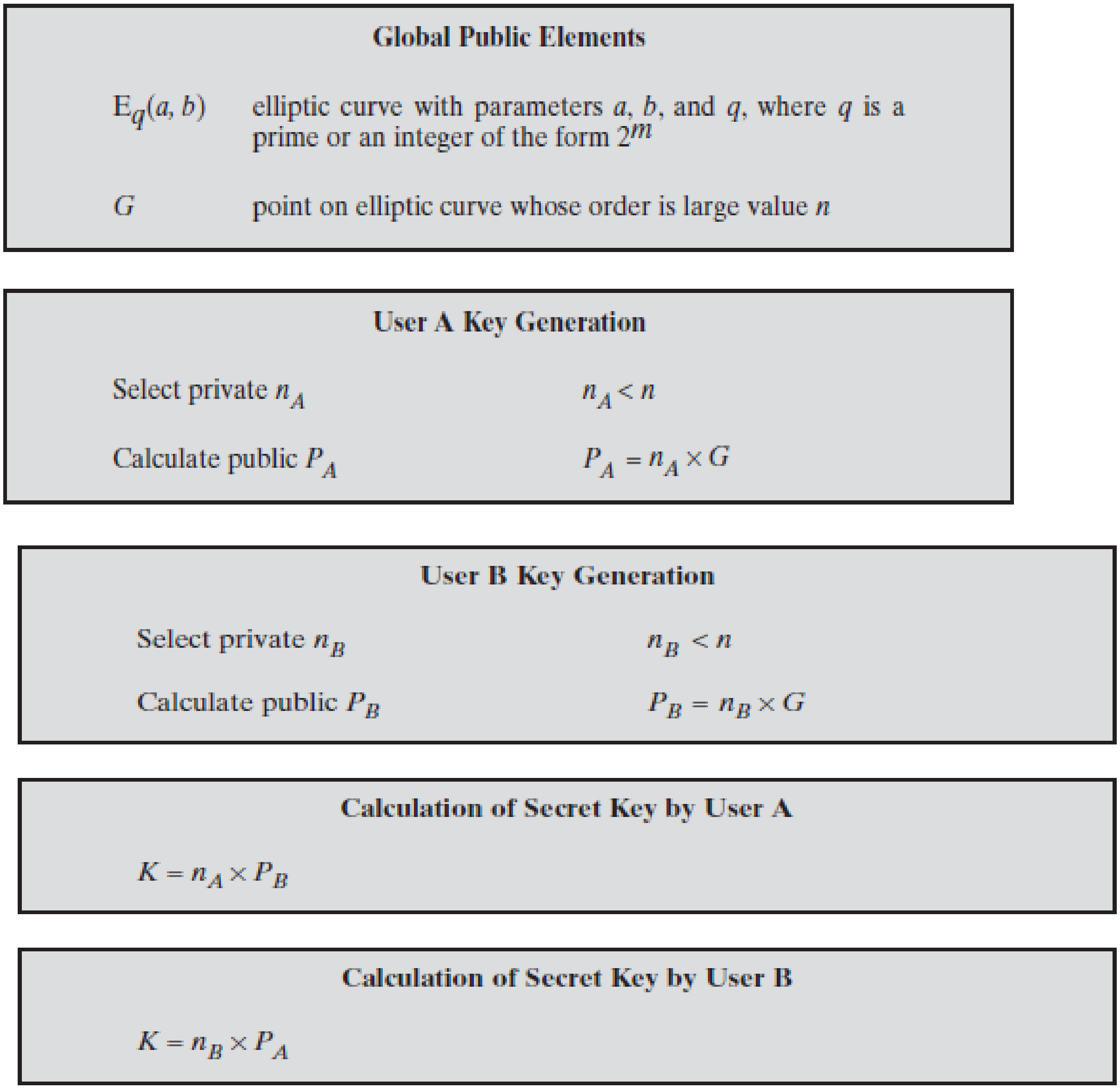
ECDH provides a secure method for two parties to agree on a shared secret key over an insecure channel without directly exchanging the secret. It is widely used in applications where secure key exchange is required, such as secure communication protocols and establishing secure connections in TLS/SSL.

22.11 Terminal Questions

1. Demonstrate Elliptic curve Diffie-Hellman Key Exchange Algorithm.
2. Illustrate Elliptic curve arithmetic over prime curves ***GF(2^m).***

22.12 Answer Key

1. The Diffie-Hellman key exchange algorithm can be adapted to use elliptic curve cryptography (ECC) instead of traditional modular arithmetic. This variant is called Elliptic Curve Diffie-Hellman (ECDH) key exchange. Here's how ECDH works::



Global Public Elements

$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation

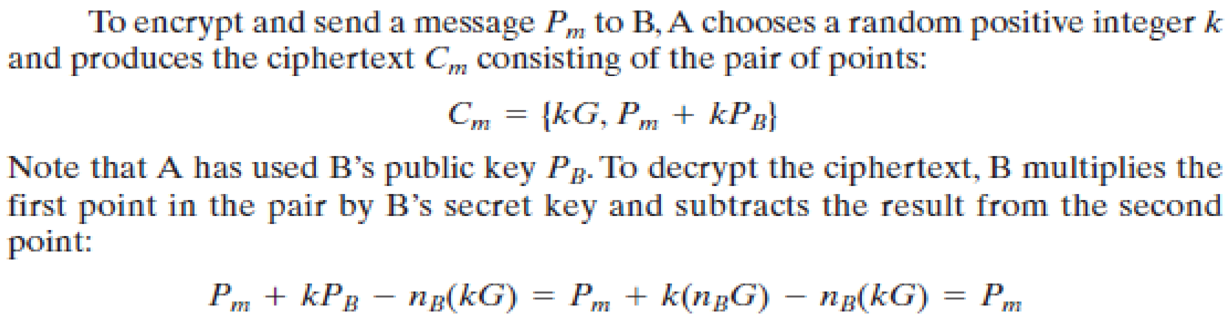
Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$



To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

2. ***<u>Elliptic Curve Arithmetic- Binary Curves GF(2^m)</u>***

- **Curve Equation:**

A binary curve is defined by an equation in the form y^2 + xy = x^3 + ax^2 + b, where a and b are coefficients, and the arithmetic is performed over a finite field of characteristic 2. The equation represents points (x, y) on the curve that satisfy the equation, along with a point at infinity, denoted as O.

- **Negative of a Point:** If A = (x_1, y_1) then –A= (x_1, $x_{1+}y_{1 \text{ mod}}$ p)
- **Point Addition:**

Given two points A = (x_1, y_1) and B = (x_2, y_2) on the curve, the sum C = A + B= (x_3, y_3) is computed.

$x_{3 =}$ $\lambda^2 + \lambda {}_{+} x_1 + x_2 + a$

$y_{3 =}$ $(\lambda(x_1+x_3)+x_3+ y_1$

$\lambda= (y_2+y_1)/ (x_2+x_1)$ mod p

- **Point Multiplication:** It is repeated addition. 3A=A+A+A

$x_{3 =}$ $\lambda^2 + \lambda + a$

22.13 Case Studies: NA

22.14 Answer Key

Self-Assessment Questions

1. a) Binary digits
2. d) The field size
3. b) x3 = s^2 + s + x1 + x2 + a
4. b) Binary curves have more efficient algorithms

5. b) Fast computations
6. b) Finite fields
7. a) Elliptic curve discrete logarithm problem
8. b) Elliptic curve point
9. a) Private key
10. a) Smaller key sizes for equivalent security
11. a)Elliptic curves over finite fields of the form GF(2^m).
12. d) All of the above
13. d)All of the above.
14. a)Binary curves are considered to be as secure as prime curves, if not more secure.
15. d)All of the above.
16. a) It uses smaller key sizes to achieve the same level of security.
17. d) Bob sends his public key to Alice.
18. b) 256 bits.
19. d)All of the above.
20. b) It requires more specialized hardware to implement.

22.15 Glossary

ECC – Elliptic Curve Cryptography

ECDH - Elliptic Curve Diffie-Hellman Key Exchange

22.16 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm's, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

3. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

4. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

22.17 Keywords

Elliptic Curve Arithmetic, Elliptic Curve Cryptography

SESSION: 23

ELLIPTIC CURVE CRYPTOGRAPHY

23.1 Aim

To illustrate concept and equations of Elliptic Curve Arithmetic & cryptography.

23.2 Instructional Objectives

The objective of this session is to introduce the basic concepts of Elliptic Curves. It provides the necessary theoretical background and summarizes properties of Abelian Group. This session further allows students to apply Elliptic curve arithmetic over prime curves and binary curves. This session also demonstrates Elliptic curve cryptography.

23.3 Learning Outcomes

At the end of this session, students are expected to know
Apply Elliptic Curve Arithmetic Binary Curves
Illustrates Elliptic Curve Diffie-Hellman Key Exchange Algorithm.

23.4 Module Description

The objective of this module is to apply Public-key cryptography algorithms and analyze various attacks possible on these algorithms.

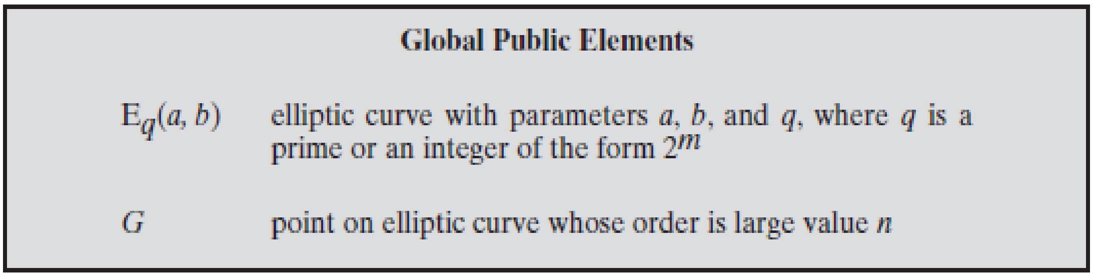
23.5 Session Introduction

This Session provides an overview of Elliptic curves. A number of elliptic curve cryptography (ECC) techniques, such as key exchange, encryption, and digital signature, can be created using elliptic curve arithmetic are discussed. The usage of an elliptic curve equation over a finite field Zp and GF(2^m) is required for elliptic curve arithmetic in the context of ECC. The equation's variables and coefficients are components of a finite field.

23.6 Session Description

23.6.1 ECC Diffie-Hellman Key Exchange

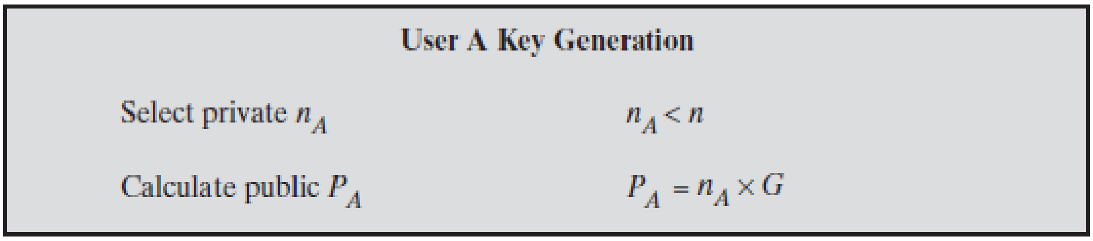
The Diffie-Hellman key exchange algorithm can be adapted to use elliptic curve cryptography (ECC) instead of traditional modular arithmetic. This variant is called Elliptic Curve Diffie-Hellman (ECDH) key exchange. Here's how ECDH works::



Global Public Elements

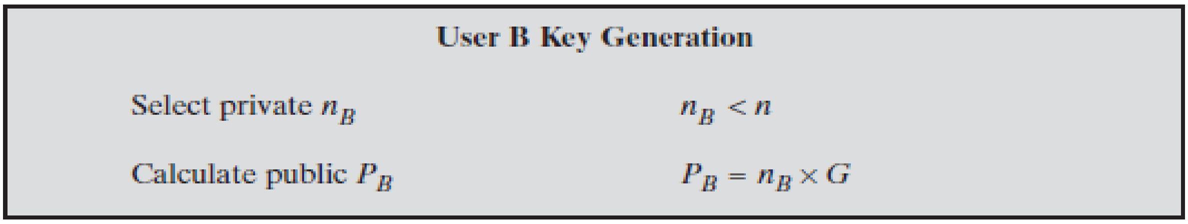
$E_q(a, b)$ elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m

G point on elliptic curve whose order is large value n



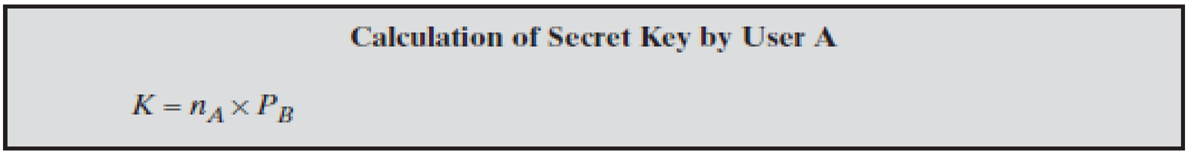
User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$



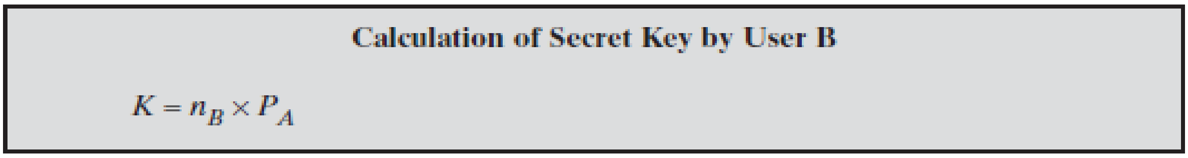
User B Key Generation

Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$



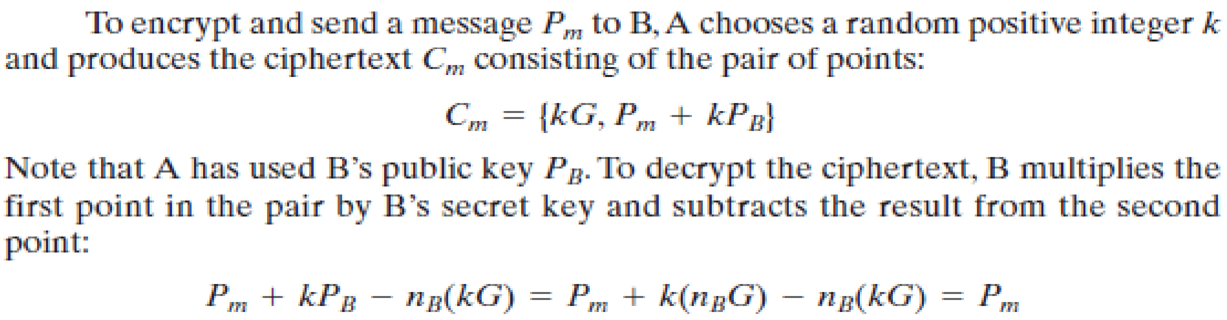
Calculation of Secret Key by User A

$K = n_A \times P_B$



Calculation of Secret Key by User B

$K = n_B \times P_A$



To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

Figure 23.1 ECC Diffie-Hellman Key Exchange Algorithm

Note: Copyrights of this figure are reserved for original author

23.7 Activities (Problem Solving): NA

23.8 Examples : NA

23.7 Table Numbering: NA

23.8 Figures with Captions

Figure 23.1 ECC Diffie-Hellman Key Exchange Algorithm

23.9 Self Assessment Questions

1. Elliptic curve cryptography is based on the algebraic structure of:

a) Prime numbers

b) Finite fields

c) Binary numbers

d) Quadratic equations

2. The security of elliptic curve cryptography is based on the difficulty of solving the:

a) Elliptic curve discrete logarithm problem

b) Elliptic curve factorization problem

c) Elliptic curve prime factor problem

d) Elliptic curve modular inverse problem

3. In elliptic curve cryptography, the private key is a randomly chosen:

a) Prime number

b) Elliptic curve point

c) Bit string

d) Encryption key

4. The public key in elliptic curve cryptography is derived from the:

a) Private key

b) Hash function

c) Random number generator

d) Diffie-Hellman algorithm

5. The main advantage of elliptic curve cryptography compared to traditional public-key cryptography is:

a) Smaller key sizes for equivalent security

b) Faster encryption and decryption algorithms

c) Stronger resistance against attacks

d) Simpler key management and distribution

Answers:

1. b) Finite fields

2. a) Elliptic curve discrete logarithm problem

3. b) Elliptic curve point

4. a) Private key

5. a) Smaller key sizes for equivalent security

23.10 Summary

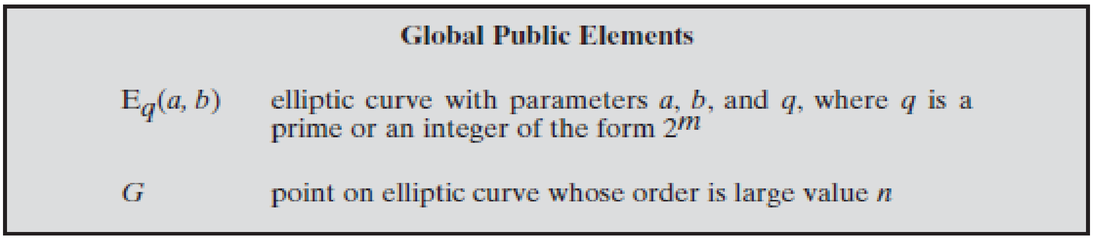
ECDH provides a secure method for two parties to agree on a shared secret key over an insecure channel without directly exchanging the secret. It is widely used in applications where secure key exchange is required, such as secure communication protocols and establishing secure connections in TLS/SSL.

23.11 Terminal Questions

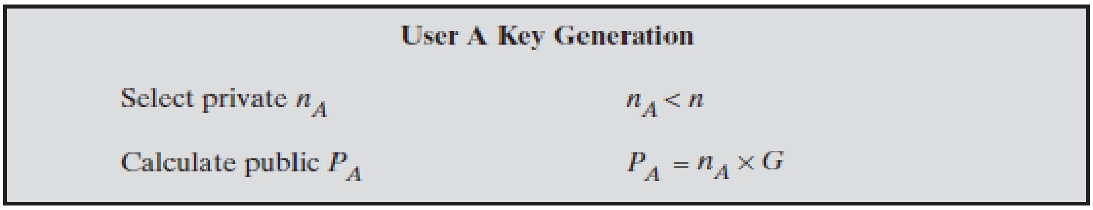
1. Demonstrate Elliptic curve Diffie-Hellman Key Exchange Algorithm.

23.12 Answer Key

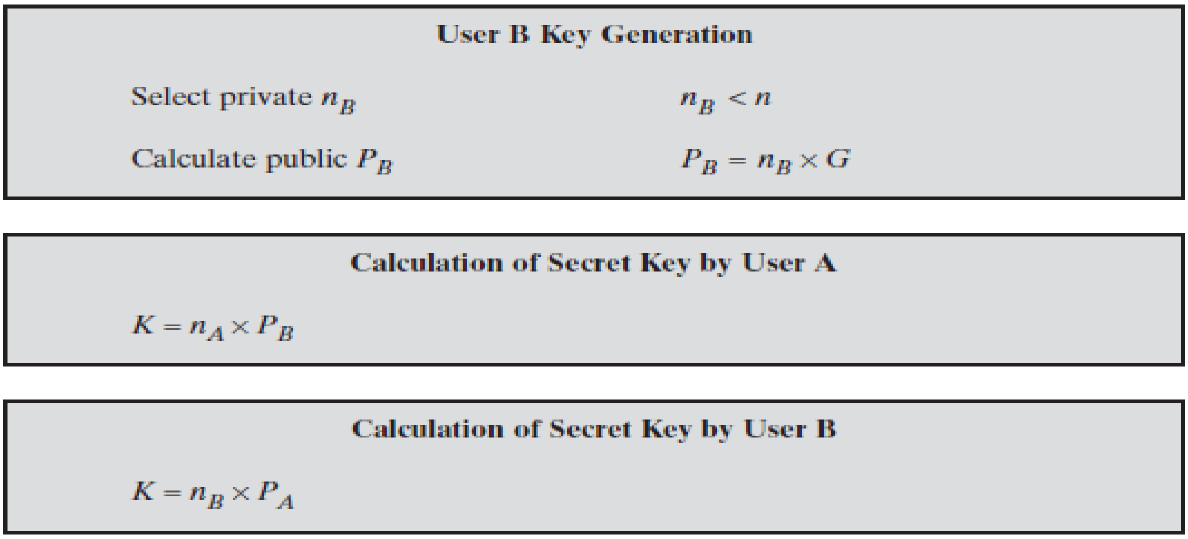
1. The Diffie-Hellman key exchange algorithm can be adapted to use elliptic curve cryptography (ECC) instead of traditional modular arithmetic. This variant is called Elliptic Curve Diffie-Hellman (ECDH) key exchange. Here's how ECDH works::



Global Public Elements	
$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n



User A Key Generation	
Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$



User B Key Generation

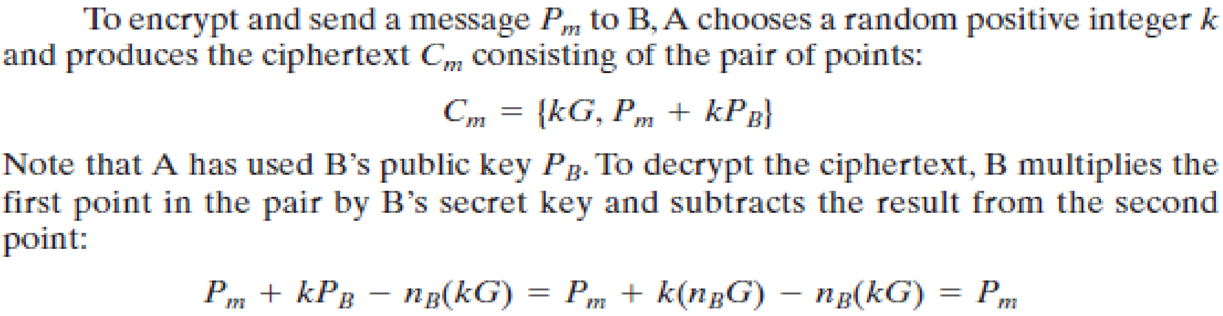
Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$



To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's secret key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

23.13 Case Studies: NA

23.14 Glossary

ECDH - Elliptic Curve Diffie-Hellman Key Exchange

23.15 References

1. Cryptography and Network Security Principles and Practice, by William stallings, Pearson, 5th edition.

2. Applied Cryptography: Protocols, Algorithm's, and Source Code in C, by Bruce Schneier, Second Edition, John Wiley & Sons, Inc., 2015

Sites and Web links:

1. Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering, by Hamid R. Nemati and Li Yang, IGI Global, 2011

2. Forouzon B, "Cryptography and Network Security," Indian Edition, TMH (2010).

23.16 Keywords

Elliptic Curve Arithmetic, Elliptic Curve Cryptography.