



Department of

CSE

CRYPTANALYSIS & CYBER
DEFENSE

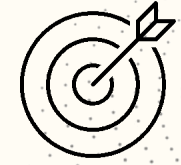
21CS3041RA

Topic:

PRINCIPLES OF PUBLIC
KEY CRYPTOSYSTEMS &
RSA ALGORITHM

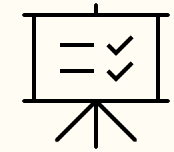
Session -17

AIM OF THE SESSION



To familiarize students with the basic concepts of Public-Key Cryptosystems and RSA algorithms

INSTRUCTIONAL OBJECTIVES



This Session is designed to:

Demonstrate Principles of Public Key Cryptosystems & RSA Algorithm

LEARNING OUTCOMES



At the end of this session, you should be able to:

1. Define Public Key Cryptosystems
2. List out applications of Principles of Public Key Cryptosystems
3. Summarize Principles of Public Key Cryptosystems
4. Apply RSA Algorithm for various values of plaintext
5. Analyze attacks on RSA Algorithm

This Session provides an overview of public-key cryptography. Much of the theory of public-key cryptosystems is based on number theory. Public-key algorithms are based on mathematical functions rather than on substitution and permutation. Public-key cryptography is asymmetric, involving the use of two separate keys, in contrast to symmetric encryption, which uses only one key. The use of two keys has profound consequences in the areas of confidentiality, key distribution, and authentication. One such example of public-key cryptosystems is RSA Algorithm.

Ingredients of Public Key Cryptosystems /Asymmetric Encryption

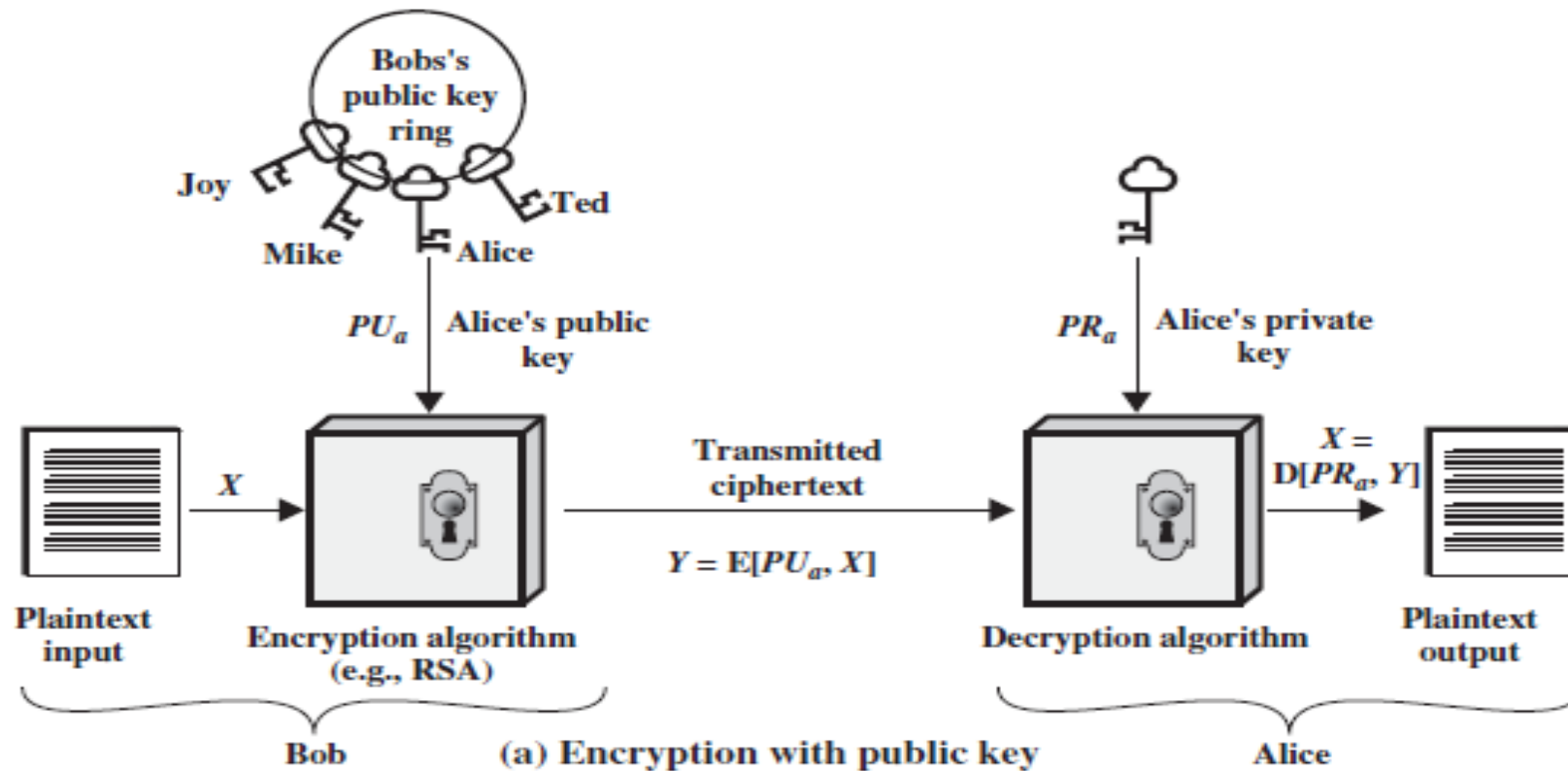
Public Key Encryption (Asymmetric)



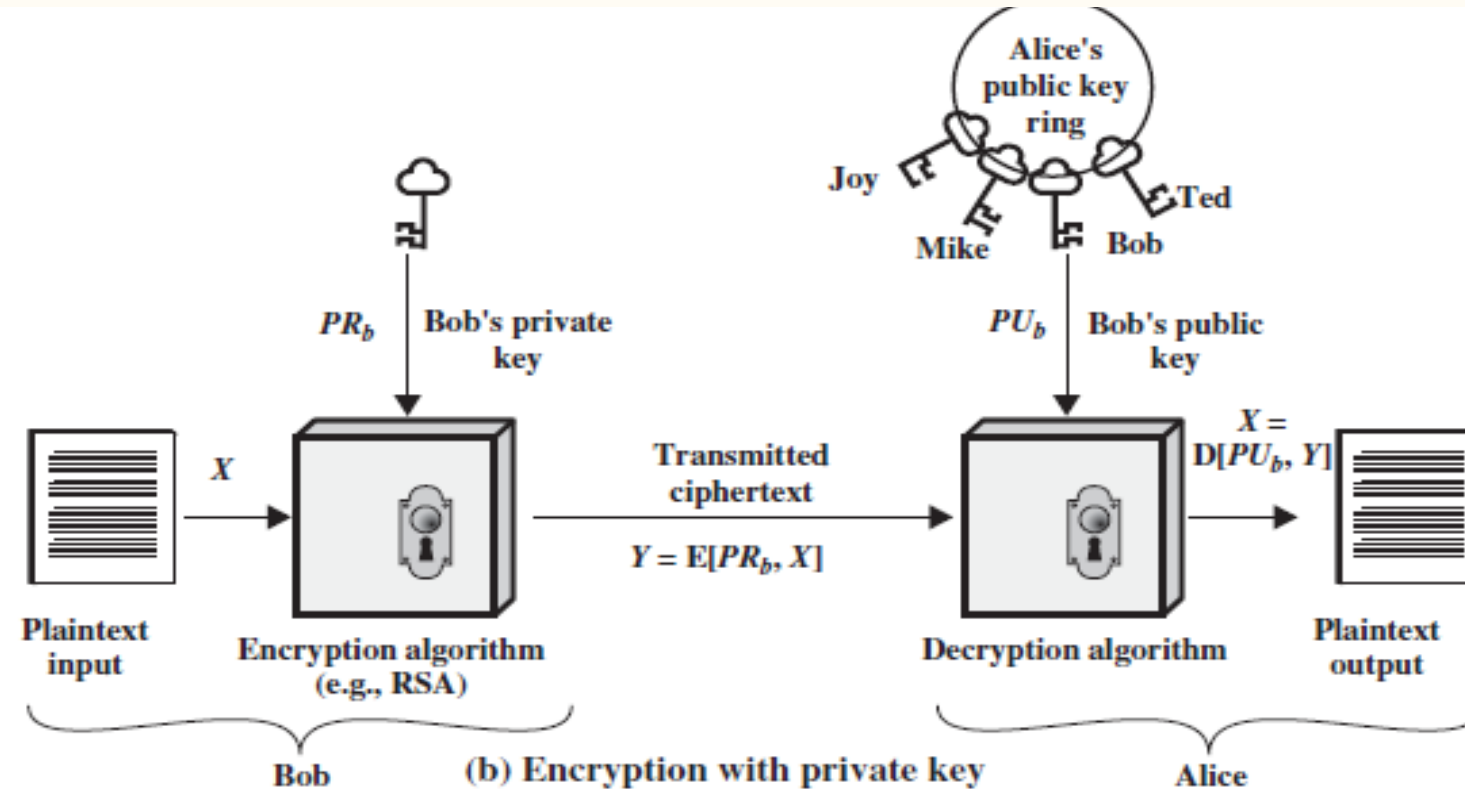
Ingredients of Public Key Cryptosystems /Asymmetric Encryption

- Ø Public Key
- Ø Private Key
- Ø Encryption Algorithm
- Ø Key Generation Algorithm
- Ø Decryption Algorithm

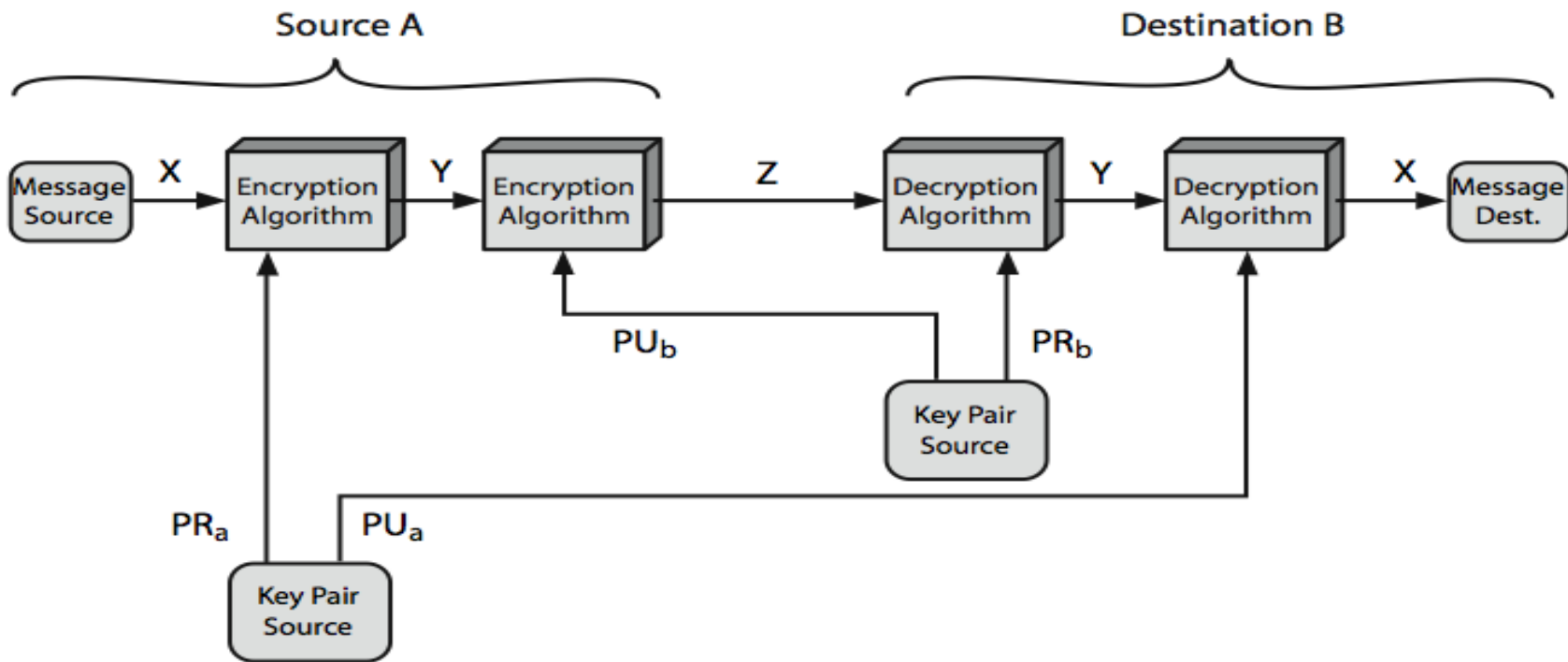
Public Key Cryptosystems for Confidentiality



Public Key Cryptosystems for Authentication



Public Key Cryptosystems for Authentication & Confidentiality



Characteristics of Public Key Cryptography

- It should be computationally infeasible to find the private key by knowing the public key and the algorithm.
- It is computationally feasible to encrypt the plain text when the encryption key is known. Similarly, it is computationally feasible to decrypt the cipher text when the decryption key is known.
- One of the two related keys can be used for encryption, and the other one for decryption.

Symmetric Key Cryptography & Public Key Cryptography Comparision

Conventional Encryption	Public-Key Encryption
<i>Needed to Work:</i> <ol style="list-style-type: none">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. <i>Needed for Security:</i> <ol style="list-style-type: none">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.	<i>Needed to Work:</i> <ol style="list-style-type: none">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). <i>Needed for Security:</i> <ol style="list-style-type: none">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.

Applications of Public Key Cryptography

- **Encryption /decryption:** The sender encrypts a message with the recipient's public key.
- **Digital signature:** The sender "signs" a message with its private key. Signing is achieved by a cryptographic algorithm applied to the message or to a small block of data that is a function of the message.
- **Key exchange:** Two sides cooperate to exchange a session key. Several different approaches are possible, involving the private key(s) of one or both parties.

- This algorithm is developed by Ronrivest, Shamir, ademan in 1977.
- It is based on Prime numbers, Exponentiation & Factorization.
- It is a block cipher in which Plaintext/Ciphertext pairs are between 0 and $n-1$ for oe n .
- Size of n is 1024 bits.



RSA Algorithm

Key Generation Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
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:	$C = M^e \pmod{n}$

Decryption by Alice with Alice's Public Key

Ciphertext:	C
Plaintext:	$M = C^d \pmod{n}$



RSA Algorithm - Example

Key Generation Alice

$p = 17; q = 11$

calculate $n = p \times q = 17 \times 11 = 187$

calculate $\phi(n) = (p-1) \times (q-1)$
 $= (17-1) \times (11-1)$
 $= 16 \times 10 = 160$

Select $e, \text{gcd}(\phi(n), e) = 1$
 $\text{gcd}(160, 7) = 1$
 e is chosen on trial & error basis.

Calculate $d \equiv e^{-1} \pmod{160}$
i.e., $(d \times e) \pmod{160} = 1$
 d is calculated on trial & error basis.
 $d = 23$

$(23 \times 7) \pmod{160} = 161 \pmod{160} = 1$

Public key $Pu = \{7, 187\}$
Private key $Pr = \{23, 187\}$



RSA Algorithm - Example

Encryption By Bob With Alice's Public Key

Plaintext $M=8$

Ciphertext $C = M^e \bmod n$

$$= 8^3 \bmod 187$$

$$= (8 \bmod 187) \times (8^2 \bmod 187)$$

$$= (8 \bmod 187) \times 64 \bmod 187$$

$$= (512 \bmod 187) \times 8 \bmod 187$$

$$= (138 \times 8) \bmod 187$$

$$= 1104 \bmod 187 = 134$$

Decryption By Alice With Its Own Private Key

Ciphertext $C=134$

Plaintext $M = C^d \bmod n$

$$= 134^{23} \bmod 187$$

$$= ((134 \bmod 187) \times (134^2 \bmod 187) \times (134^4 \bmod 187) \times (134^8 \bmod 187) \times (134^8 \bmod 187)) \bmod 187$$

Attacks on RSA algorithm

- Possible approaches to attack RSA are:
 - Ø Brute force key search
 - Ø Mathematical attacks (factoring n)
 - Ø Chosen ciphertext attacks
 - Ø Timing attacks

Attacks on RSA algorithm

- **Brute force key search**

- Ø Try all possible keys in hit and trial approach

- **Mathematical attacks (factoring n)**

Mathematical approach takes 3 forms:

- Ø factor $n = p \cdot q$, hence compute $\phi(n)$ and then d

- Ø determine $\phi(n)$ directly and compute d

- Ø find d directly

- Currently assume 1024–2048 bit RSA is secure

Attacks on RSA algorithm

- **Chosen ciphertext attacks**

Attackers chooses ciphertexts & gets decrypted plaintext back. Can counter with random pad of plaintext.

2. Timing attacks

- Developed by Paul Kocher in mid-1990's
- Exploit timing variations in operations
 - Ø eg. multiplying by small vs large number
- Infer operand size based on time taken
- RSA exploits time taken in exponentiation
- Countermeasures
 - Ø use constant exponentiation time
 - Ø add random delays
 - Ø blind values used in calculations

SUMMARY

These principles of public key cryptography and are instrumental in achieving secure communication, confidentiality, integrity, authentication, and non-repudiation of digital information. In summary, conventional encryption (symmetric encryption) is faster and more efficient, but it requires securely sharing a secret key. Asymmetric encryption provides a more secure way of key exchange and communication, but it is slower and computationally more expensive. Public key cryptography versatility and strong security guarantees make it a fundamental building block in modern cryptographic systems and secure communication protocols. It's worth noting that while RSA is a powerful encryption algorithm, its security relies on the proper generation and management of keys, appropriate key sizes, and protection against various attacks like timing attacks and side-channel attacks.

SELF-ASSESSMENT QUESTIONS

1. What are the principal elements of a public-key cryptosystem?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

2. What are three broad categories of applications of public-key cryptosystems?

- (a) Encryption
- (b) Digital Signature
- (c) Key Exchange
- (d) All the above

SELF-ASSESSMENT QUESTIONS

1. What is $\{e,n\}$ in RS Algorithm?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

1. What is $\{d,n\}$ in RS Algorithm?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

1. Summarize Public key Cryptosystems
2. List out applications of Public key Cryptosystems
3. Distinguish Symmetric Encryption and Public key Cryptosystems
4. Summarize RSA Algorithm.
5. Perform encryption and decryption using the RSA algorithm for the following: $p = 3$; $q = 11$, $e = 7$; $M = 5$.
6. Analyze attacks on RSA Algorithm.

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



Team – Course Name



Department of

CSE

CRYPTANALYSIS & CYBER
DEFENSE

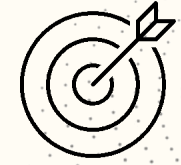
21CS3041RA

Topic:

RSA ALGORITHM

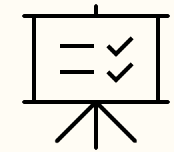
Session -18

AIM OF THE SESSION



To familiarize students with the basic concepts of Public-Key Cryptosystems and RSA algorithms

INSTRUCTIONAL OBJECTIVES



This Session is designed to:
Demonstrate RSA Algorithm

LEARNING OUTCOMES



At the end of this session, you should be able to:

1. Apply RSA Algorithm for a given value of plaintext.
2. Analyze attacks on RSA Algorithm

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.

- This algorithm is developed by Ronrivest, Shamir, ademan in 1977.
- It is based on Prime numbers, Exponentiation & Factorization.
- It is a block cipher in which Plaintext/Ciphertext pairs are between 0 and $n-1$ for oe n .
- Size of n is 1024 bits.



RSA Algorithm

Key Generation Alice

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
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:	$M = C^d \bmod n$



RSA Algorithm - Example

Key Generation Alice

$p = 17; q = 11$

calculate $n = p \times q = 17 \times 11 = 187$

calculate $\phi(n) = (p-1) \times (q-1)$
 $= (17-1) \times (11-1)$
 $= 16 \times 10 = 160$

Select $e, \text{gcd}(\phi(n), e) = 1$
 $\text{gcd}(160, 7) = 1$
 e is chosen on trial & error basis.

Calculate $d \equiv e^{-1} \pmod{160}$
i.e., $(d \times e) \pmod{160} = 1$
 d is calculated on trial & error basis.
 $d = 23$

$(23 \times 7) \pmod{160} = 161 \pmod{160} = 1$

Public key $PU = \{7, 187\}$
Private key $PR = \{23, 187\}$



RSA Algorithm - Example

Encryption By Bob With Alice's Public Key

Plaintext $M = 8$

Ciphertext $C = M^e \bmod n$

$$= 8^3 \bmod 187$$

$$= (8 \bmod 187) \times (8^2 \bmod 187)$$

$$= (8 \bmod 187) \times 64 \bmod 187$$

$$= (512 \bmod 187) \times 8 \bmod 187$$

$$= (138 \times 8) \bmod 187$$

$$= 1104 \bmod 187 = 134$$

Decryption By Alice With Its Own Private Key

Ciphertext $C = 134$

Plaintext $M = C^d \bmod n$

$$= 134^{23} \bmod 187$$

$$= (134 \bmod 187) \times (134^2 \bmod 187)$$

$$\times (134^4 \bmod 187) \times (134^8 \bmod 187)$$

$$\times (134^8 \bmod 187)$$

Attacks on RSA algorithm

- Possible approaches to attack RSA are:
 - Ø Brute force key search
 - Ø Mathematical attacks (factoring n)
 - Ø Chosen ciphertext attacks
 - Ø Timing attacks

Attacks on RSA algorithm

- **Brute force key search**

- Ø Try all possible keys in hit and trial approach

- **Mathematical attacks (factoring n)**

Mathematical approach takes 3 forms:

- Ø factor $n = p \cdot q$, hence compute $\phi(n)$ and then d

- Ø determine $\phi(n)$ directly and compute d

- Ø find d directly

- Currently assume 1024–2048 bit RSA is secure

Attacks on RSA algorithm

- **Chosen ciphertext attacks**

Attackers chooses ciphertexts & gets decrypted plaintext back. Can counter with random pad of plaintext.

2. Timing attacks

- Developed by Paul Kocher in mid-1990's
- Exploit timing variations in operations
 - Ø eg. multiplying by small vs large number
- Infer operand size based on time taken
- RSA exploits time taken in exponentiation
- Countermeasures
 - Ø use constant exponentiation time
 - Ø add random delays
 - Ø blind values used in calculations

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.

SELF-ASSESSMENT QUESTIONS

1. What are the principal elements of a public-key cryptosystem?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

2. What are three broad categories of applications of public-key cryptosystems?

- (a) Encryption
- (b) Digital Signature
- (c) Key Exchange
- (d) All the above

SELF-ASSESSMENT QUESTIONS

1. What is $\{e,n\}$ in RS Algorithm?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

1. What is $\{d,n\}$ in RS Algorithm?

- (a) Public Key
- (b) Private Key
- (c) Both A & B
- (d) None

1. Summarize RSA Algorithm.
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.

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



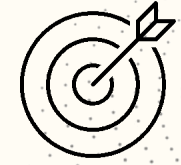
Team – Cryptanalysis & Cyber Defense



Department of
CSE
CRYPTANALYSIS & CYBER
DEFENSE
21CS3041RA
Topic:
DIFFIE-HELLMAN KEY
EXCHANGE
ALGORITHM

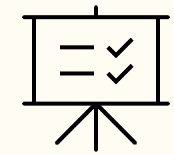
Session – 19

AIM OF THE SESSION



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

INSTRUCTIONAL OBJECTIVES



This Session is designed to:
demonstrate how a secret key is exchanged between source and destinations.

LEARNING OUTCOMES



At the end of this session, you should be able to:

1. Apply Diffie-Hellman & Elgama Algorithms on different plaintexts.
2. Analyze Man-in-the-Middle attack on Diffie-Hellman Algorithm

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,

- Diffie & Hellman in 1976 proposed a public key cryptosystem for creating a shared secret key.
- The value of key depends on the private and public keys of the two participants.
- It is based on exponentiation function
- The security relies on the difficulty of factoring

Diffie-Hellman Key Exchange Algorithm

Global Public Elements

q prime number
 α $\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A $X_A < q$
Calculate public Y_A $Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B $X_B < q$
Calculate public Y_B $Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A

$$K = (Y_B)^{X_A} \bmod q$$

Calculation of Secret Key by User B

$$K = (Y_A)^{X_B} \bmod q$$

Primitive root example

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.

3^1	=	3	\equiv	3 (mod 7)
3^2	=	9	\equiv	2 (mod 7)
3^3	=	27	\equiv	6 (mod 7)
3^4	=	81	\equiv	4 (mod 7)
3^5	=	243	\equiv	5 (mod 7)
3^6	=	729	\equiv	1 (mod 7)



Diffie-Hellman Key Exchange-Example & Proof that a Secret Key is Exchanged Between Source & Destination

Global Public Elements

$$q = 353$$
$$g = 3$$

USER A Key Generation

Private key $x_A = 97$

Calculate public key $y_A = g^{x_A} \bmod q$

$$y_A = 3^{97} \bmod 353$$
$$= 40$$

USER B Key Generation

Private key $x_B = 233$

Calculate public key $y_B = g^{x_B} \bmod q$

$$y_B = 3^{233} \bmod 353$$
$$= 248$$

Secret key of USER A

$$K = (y_B)^{x_A} \bmod q$$
$$= (248)^{97} \bmod 353 = 160$$

Secret key of USER B

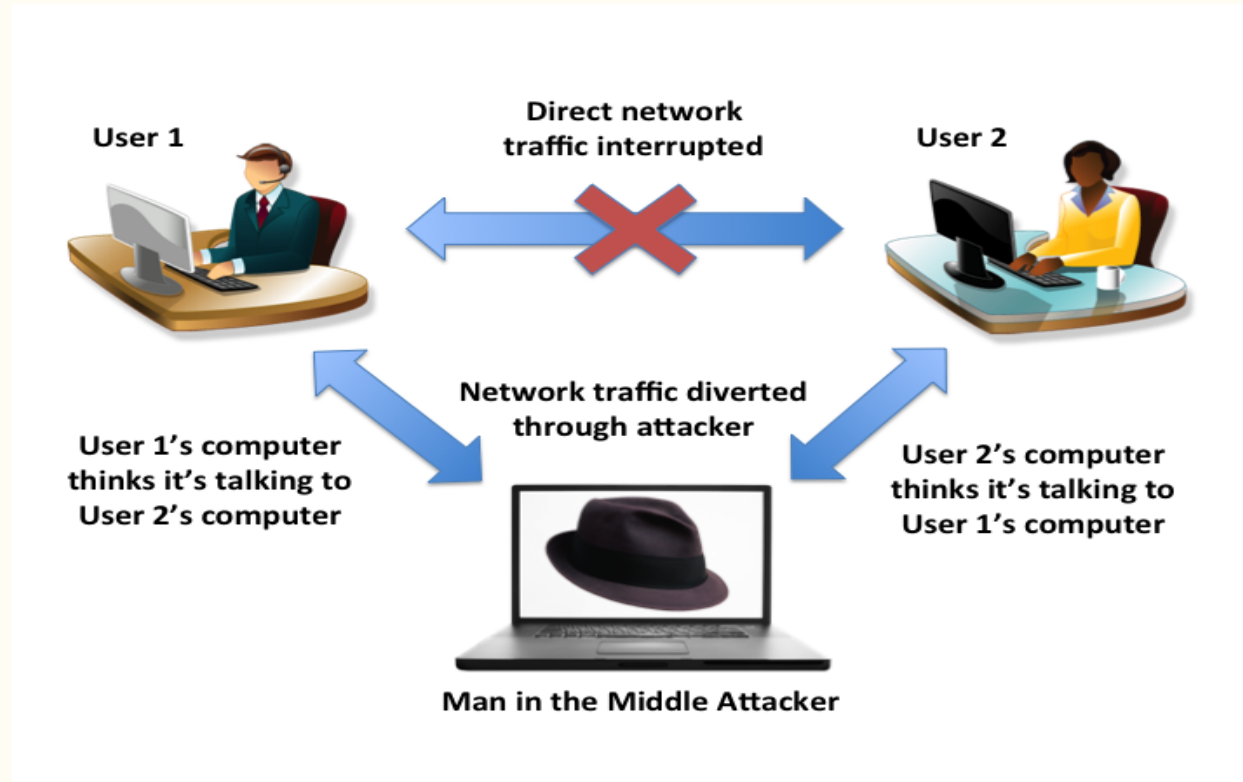
$$K = (y_A)^{x_B} \bmod q = (40)^{233} \bmod 353$$
$$= 160$$

Diffie-Hellman Key Exchange–Mathematical Proof that a Secret Key is Exchanged Between Source & Destination

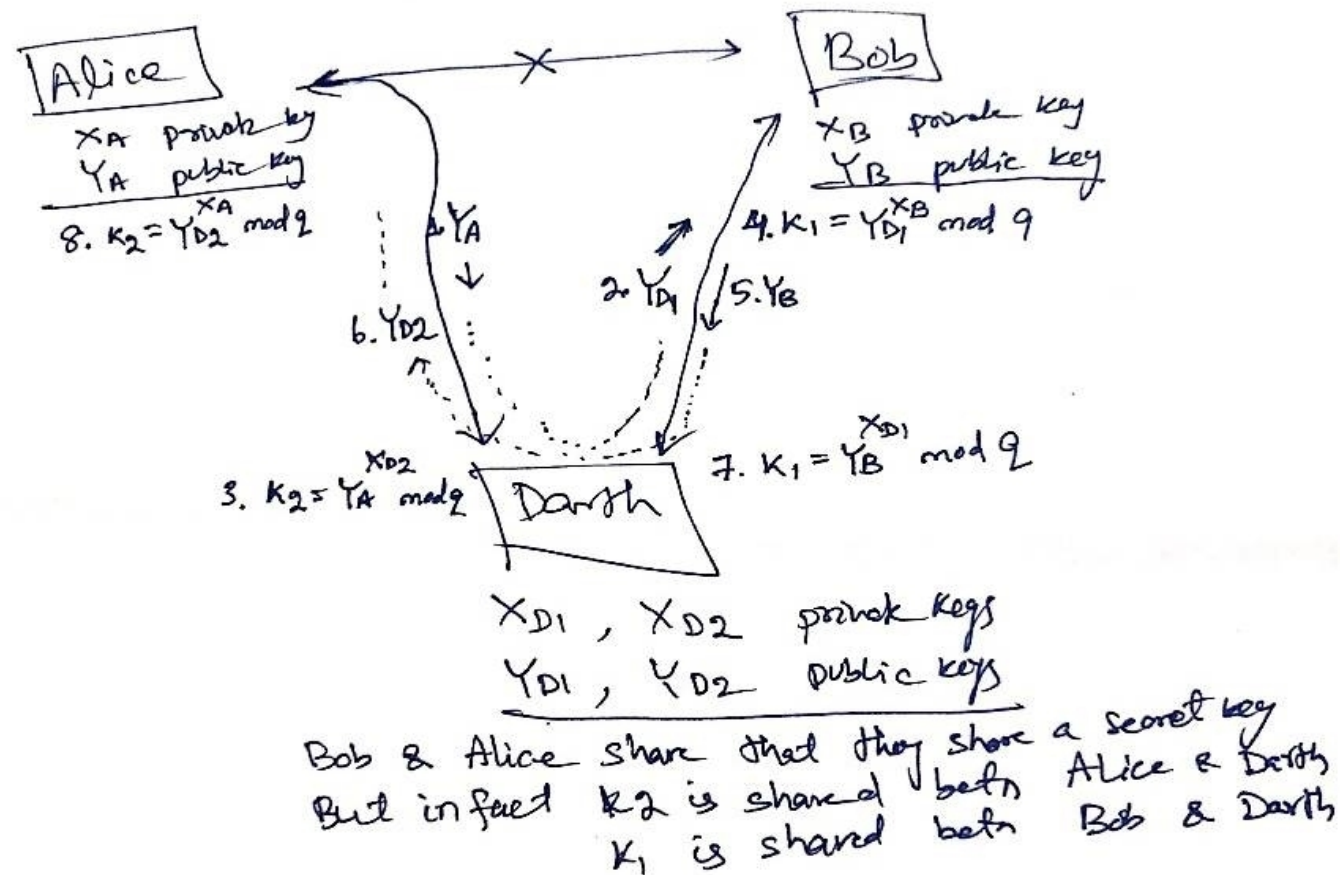
$$\begin{aligned} K &= (Y_B)^{X_A} \bmod q \\ &= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \\ &= (\alpha^{X_B})^{X_A} \bmod q \\ &= \alpha^{X_B X_A} \bmod q \\ &= (\alpha^{X_A})^{X_B} \bmod q \\ &= (\alpha^{X_A} \bmod q)^{X_B} \bmod q \\ &= (Y_A)^{X_B} \bmod q \end{aligned}$$

by the rules of modular arithmetic

Man-in-the-Middle Attack(MITM)



Man-in-the-Middle Attack(MITM)



Man-in-the-Middle Attack(MITM)

1. DARTH prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}
 2. Alice transmits Y_A to Bob
 3. DARTH intercepts Y_A and transmits Y_{D1} to Bob. DARTH also calculates $K2 = (Y_A)^{X_{D2}} \bmod q$
 4. Bob receives Y_{D1} and calculates $K1 = (Y_{D1})^{X_B} \bmod q$
 5. Bob transmits Y_B to Alice
 6. DARTH intercepts Y_B and transmits Y_{D2} to Alice. DARTH calculates $K1 = (Y_B)^{X_{D1}} \bmod q$
 7. Alice receives Y_{D2} and calculates $K2 = (Y_{D2})^{X_A} \bmod q$
- 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 $k2$.

Man-in-the-Middle Attack(MITM)

- The future communication between Bob and Alice is compromised in the following way:
 1. Alice sends an encrypted message M: $E(K_2, M)$.
 2. Darth intercepts the encrypted message and decrypts it, to recover M.
 3. Darth sends Bob $E(K_1, M)$ or $E(K_1, M')$, where M' is any message.
- In the first case, Darth simply wants to eavesdrop on the communication without altering it. In the second case, Darth wants to modify the message going to Bob.
- The key exchange protocol is vulnerable to such an attack because it does not authenticate the participants. This vulnerability can be overcome with the use of digital signatures and public-key certificates.

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

SELF-ASSESSMENT QUESTIONS

1. Identify the name of the algorithm in which a secret key is exchanged between source & destination.

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

2. Man-in-the-Middle attack is possible on which algorithm?

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

SELF-ASSESSMENT QUESTIONS

3. Identify Asymmetric encryption algorithm among the following.

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

4. Man-in-the-Middle attack is possible on which algorithm?

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

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?

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



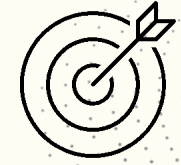
Team – Cryptanalysis & Cyber Defense



Department of
CSE
**CRYPTANALYSIS & CYBER
DEFENSE**
21CS3041RA
Topic:
ELGAMAL ALGORITHM

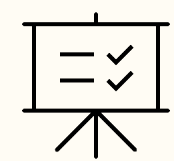
Session – 20

AIM OF THE SESSION



To familiarize students with the basic concept of Elgamal Algorithm

INSTRUCTIONAL OBJECTIVES



This Session is designed to: demonstrate Elgamal Cryptosystems.

LEARNING OUTCOMES



At the end of this session, you should be able to:

1. Apply Elgamal Algorithms on different plaintexts.

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.

Elgamal Cryptosystem

In 1984, T. Elgamal announced a public-key scheme based on discrete logarithms, closely related to the Diffie-Hellman technique.

It is used in some form in a number of standards including the digital signature standard



Elgamal Cryptosystem

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice

Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$PU = \{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key

Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

Decryption by Alice with Alice's Private Key

Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$



Elgamal Cryptosystem – Example

GLOBAL PUBLIC ELEMENTS

$$q = 19$$
$$\alpha = 10$$

Key Generation By ALICE

Select Private Key $x_A = 5$

$$\text{Calculate } y_A = \alpha^{x_A} \bmod q = 10^5 \bmod 19 = 3$$

Public Key $PU = \{q, \alpha, y_A\}$
 $= \{19, 10, 3\}$

Encryption By BOB With ALICE's Public Key

Plaintext $M = 17$

Select random integer $k = 6$

$$\text{Calculate } K = (y_A)^k \bmod q = 3^6 \bmod 19 = 729 \bmod 19 = 7$$
$$\text{Calculate } C_1 = \alpha^k \bmod q = 10^6 \bmod 19 = 11$$
$$\text{Calculate } C_2 = KM \bmod q = 7 \times 17 \bmod 19 = 119 \bmod 19 = 5$$

Ciphertext $(C_1, C_2) = (11, 5)$

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.

SELF-ASSESSMENT QUESTIONS

1. Identify the name of the algorithm in which a secret key is exchanged between source & destination.

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

2. Man-in-the-Middle attack is possible on which algorithm?

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

SELF-ASSESSMENT QUESTIONS

3. Identify Asymmetric encryption algorithm among the following.

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

4. Man-in-the-Middle attack is possible on which algorithm?

- (a) Diffie-Hellman
- (b) Elgamal
- (c) Both A & B
- (d) None

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 $\beta = \alpha^a \pmod{p}$ is Alice's public key parameter. Bob wants to send the message $M = 10$ to Alice AND SECRET KEY $K=7$.

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



Team – Cryptanalysis & Cyner Defense



Department of

CSE

CRYPTANALYSIS & CYBER

DEFENSE

21CS3041RA

Topic:

ELLIPTIC CURVE

ARITHMETIC

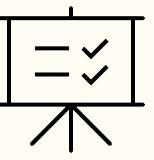
Session – 21

AIM OF THE SESSION




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

INSTRUCTIONAL OBJECTIVES



This Session is designed to: demonstrate elliptic curve arithmetic and distinguishes between prime and binary curves

LEARNING OUTCOMES



At the end of this session, you should be able to:

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

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.

An abelian group, sometimes denoted by (G, \cdot) , is a set of elements with a binary operation, denoted by \cdot , that associates to each ordered pair of elements in G an element in G , such that the following axioms are obeyed:

- | | |
|-------------------------------|---|
| (A1) Closure: | If a and b belong to G , then $a \cdot b$ is also in G . |
| (A2) Associative: | $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G . |
| (A3) Identity element: | There is an element e in G such that $a \cdot e = e \cdot a = a$ for all a in G . |
| (A4) Inverse element: | For each a in G there is an element a' in G such that $a \cdot a' = a' \cdot a = e$. |
| (A5) Commutative: | $a \cdot b = b \cdot a$ for all a, b in G . |

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

- For a prime curve over \mathbb{Z}_p , we use cubic equation in which variables & coefficients all take 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 $\text{GF}(2^m)$, the variables & coefficients all take on values in $\text{GF}(2^m)$ and calculations are performed over $\text{GF}(2^m)$. Best for h/w applications

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

1. $P + O = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, -y_P) = O$. The point $(x_P, -y_P)$ is the negative of P , denoted as $-P$. For example, in $E_{23}(1, 1)$, for $P = (13, 7)$, we have $-P = (13, -7)$. But $-7 \bmod 23 = 16$. Therefore, $-P = (13, 16)$, which is also in $E_{23}(1, 1)$.
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

where

$$\lambda = \begin{cases} \left(\frac{y_Q - y_P}{x_Q - x_P} \right) \bmod p & \text{if } P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P} \right) \bmod p & \text{if } P = Q \end{cases}$$

4. Multiplication is defined as repeated addition; for example, $4P = P + P + P + P$.

For example, let $P = (3, 10)$ and $Q = (9, 7)$ in $E_{23}(1, 1)$. Then

$$\lambda = \left(\frac{7 - 10}{9 - 3} \right) \bmod 23 = \left(\frac{-3}{6} \right) \bmod 23 = \left(\frac{-1}{2} \right) \bmod 23 = 11$$

$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$

The last step in the preceding equation involves taking the multiplicative inverse of 4 in \mathbb{Z}_{23} . This can be done using the extended Euclidean algorithm defined in Section 4.4. To confirm, note that $(6 \times 4) \bmod 23 = 24 \bmod 23 = 1$.

$$x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$$

$$y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$$

and $2P = (7, 12)$.

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

SELF-ASSESSMENT QUESTIONS

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

- (a) Closure under addition (-23, -43)
- (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

(a) s

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 .

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



Team – Cryptanalysis & Cyber Defense



Department of

CSE

CRYPTANALYSIS & CYBER

DEFENSE

21CS3041RA

Topic:

ELLIPTIC CURVE

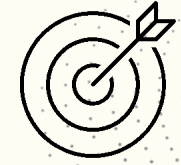
ARITHMETIC &

ELLIPTIC CURVE

CRYPTOGRAPHY

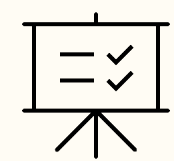
Session – 22

AIM OF THE SESSION



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

INSTRUCTIONAL OBJECTIVES



This Session is designed to: demonstrate elliptic curve arithmetic & cryptography.

LEARNING OUTCOMES



At the end of this session, you should be able to:

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

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 \mathbb{Z}_p and $\text{GF}(2^m)$ is required for elliptic curve arithmetic in the context of ECC. The equation's variables and coefficients are components of a finite field.

It can be shown that a finite abelian group can be defined based on the set $E_{2^m}(a, b)$, provided that $b \neq 0$. The rules for addition can be stated as follows. For all points $P, Q \in E_{2^m}(a, b)$:

1. $P + O = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, x_P + y_P) = O$. The point $(x_P, x_P + y_P)$ is the negative of P , which is denoted as $-P$.
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$ and $P \neq Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + x_P + x_Q + a$$

$$y_R = \lambda(x_P + x_R) + x_R + y_P$$

:

where

$$\lambda = \frac{y_Q + y_P}{x_Q + x_P}$$

4. If $P = (x_P, y_P)$ then $R = 2P = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + a$$

$$y_R = x_P^2 + (\lambda + 1x)_R$$

where

$$\lambda = x_P + \frac{y_P}{x_P}$$



Elliptic Curve Cryptography – Diffie Hellman Key Exchange

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

$$K = n_B \times P_A$$

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

SELF-ASSESSMENT QUESTIONS

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

- (a) Prime number
- (b) Elliptic curve point
- (c) Bit string
- (d) Encryption key

2. 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

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

Reference Books:

1. Cryptography and Network Security Principles and Practice, by William Stallings, Pearson, 5th edition.
2. Applied Cryptography: Protocols, Algorithms, 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).

THANK YOU



Team – Cryptanalysis & Cyber Defense