By Narendra Bohara

UNIT III: ASYMMETRIC CIPHERS

By Narendra Bohara

CONTENTS

- Number Theory: Prime Numbers, Fermat's Theorem, Euler's Theorem, Primality Testing, Miller-Rabin Algorithm, Extended Euclidean Theorem, Discrete Logarithms.
- Public Key Cryptosystems, Applications of Public Key Cryptosystems .
- Distribution of public key, Distribution of secret key by using public key cryptography.
- Diffie-Helman Key Exchange, Man-in-the-Middle Attack.
- RSA Algorithm .
- Elgamal Cryptographic System.

By Narendra Bohara

PUBLIC KEY CRYPTOSYSTEMS

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.

- It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key.

In addition, some algorithms, such as RSA, also exhibit the following characteristic.

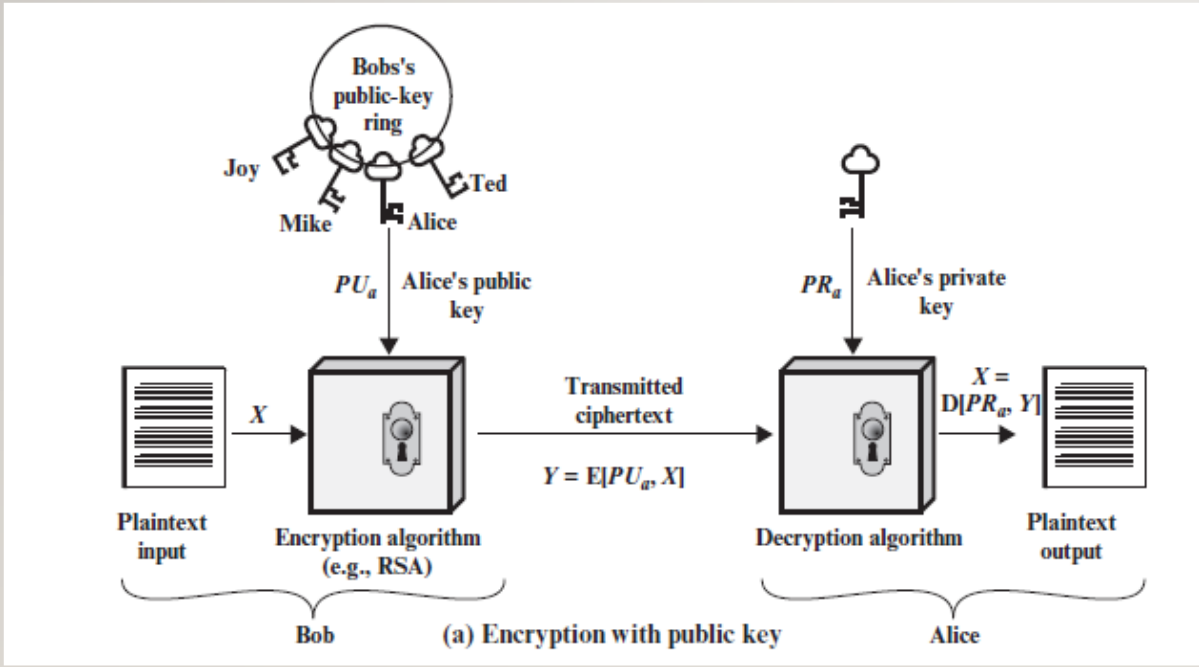
- Either of the two related keys can be used for encryption, with the other used for decryption.

By Narendra Bohara

INGREDIENTS OF PUBLIC-KEY ENCRYPTION SCHEME

- **Plaintext:** This is the readable message or data that is fed into the algorithm as input.
- **Encryption algorithm:** The encryption algorithm performs various transformations on the plaintext.
- **Public and private keys:** This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
- **Ciphertext:** This is the encrypted message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

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



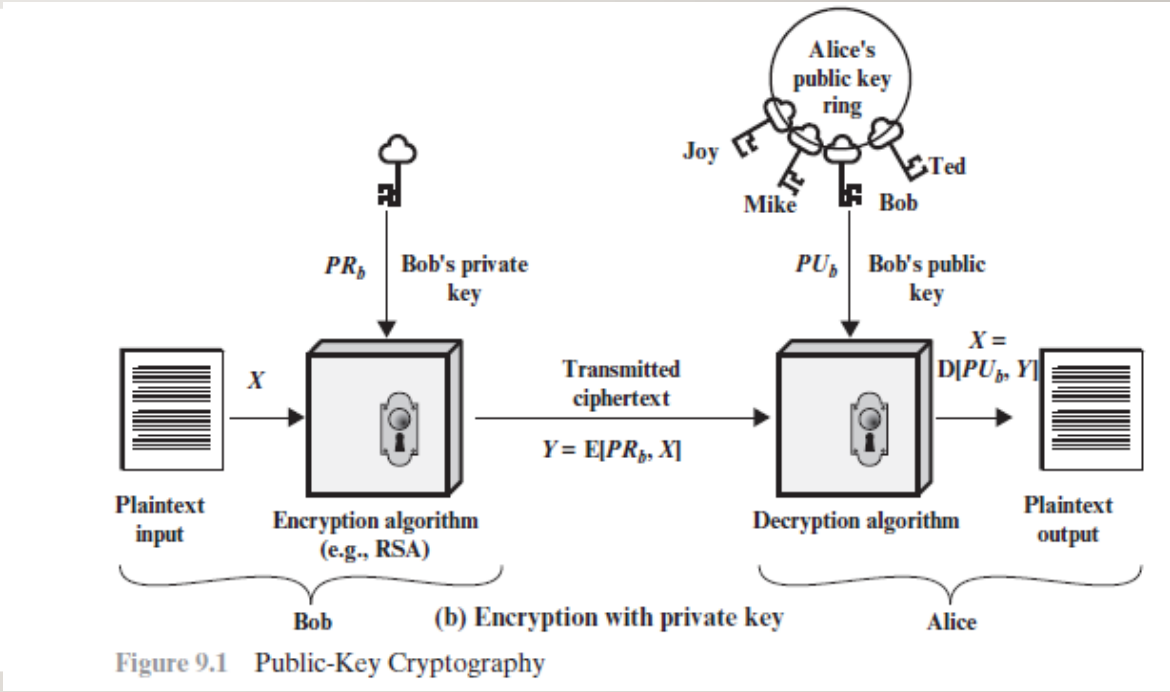


Figure 9.1 Public-Key Cryptography

By Narendra Bohara

THE ESSENTIAL STEPS

1. Each user generates a pair of keys to be used for the encryption and decryption of messages.
2. Each user places one of the two keys in a public register or other accessible file. This is the public key. The companion key is kept private.
3. If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
4. When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

CONVENTIONAL AND PUBLIC-KEY ENCRYPTION

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 the key is kept secret. 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 a related algorithm for 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 one of the keys is kept secret. 3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.

By Narendra Bohara

APPLICATIONS FOR PUBLIC-KEY CRYPTOSYSTEMS

- Public-key systems are characterized by the use of a cryptographic algorithm with two keys, one held private and one available publicly. Depending on the application, the sender uses either the sender's private key or the receiver's public key, or both, to perform some type of cryptographic function.
- we can classify the use of **public-key cryptosystems** into three categories
  - ✓ **Encryption/decryption**
  - ✓ **Digital signature**
  - ✓ **Key exchange**

By Narendra Bohara

APPLICATIONS FOR PUBLIC-KEY CRYPTOSYSTEMS

- **Encryption/decryption:** The sender encrypts a message with the recipient's public key, and the recipient decrypts the message with the recipient's private 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, which is a secret key for symmetric encryption generated for use for a particular transaction (or session) and valid for a short period of time. Several different approaches are possible, involving the private key(s) of one or both parties.

By Narendra Bohara

REQUIREMENTS FOR PUBLIC-KEY CRYPTOGRAPHY

1. It is computationally easy for a party B to generate a key pair (public key PU_b, private key PR^b).
2. It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:

$$C = E(PU_b, M)$$

3. It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message.

$$M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$$

4. It is computationally infeasible for an adversary, knowing the public key, PU_b, to determine the private key, PR_b.

By Narendra Bohara

THE RSA ALGORITHM

- One of the first public-key schemes was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT.
- **RSA** is a block cipher in which the plaintext and ciphertext are integers between 0 and *n-1* for some *n*.

By Narendra Bohara

STEPS

KEY GENERATION

1. select two prime numbers p and q and calculate their product n, which is the modulus for encryption and decryption as $n = p \times q$.
2. we need the quantity $\varphi(n)$, referred to as the Euler totient of n, which is the number of positive integers less than n and relatively prime to n as $\varphi(n) = (p - 1)(q - 1)$
3. Then select an integer e that is relatively prime to $\varphi(n)$ [i.e., the greatest common divisor of e and $\varphi(n)$ is 1] i.e. Select integer e ,gcd $(\varphi(n), e) = 1$; $1 < e < \varphi(n)$.
4. Finally, calculate d as the multiplicative inverse of e, modulo $\varphi(n)$ i,.e. ,$de \bmod \varphi(n) = 1$
5. Public key $KU = \{e, n\}$
6. Private key $KR = \{d, n\}$

By Narendra Bohara

ENCRYPTION/DECRYPTION

- Suppose that user A has published its public key and that user B wishes to send the message *M* to A.
- Then B calculates Ciphertext: $C = M^e \pmod{n}$ and transmits to A.
- On receipt of this ciphertext, user A decrypts by calculating $M = C^d \pmod{n}$.

By Narendra Bohara

EXAMPLE 1

1. Let two primes be p = 7 and q = 13. Thus, modulus n = pq = 7 x 13 = 91.
2. Select e = 5, which is a valid choice since there is no number that is common factor of 5 and $\varphi(n)$= (p − 1)(q − 1) = 6 × 12 = 72, except for 1.
3. The pair of numbers (n, e) = (91, 5) forms the public key and can be made available to anyone whom we wish to be able to send us encrypted messages.
4. Input p = 7, q = 13, and e = 5 to the Extended Euclidean Algorithm. The output will be d = 29.
5. Check that the d calculated is correct by computing de=29*5=145=1mod72.
6. Hence, public key is (91, 5) and private keys is (91, 29).

By Narendra Bohara

ENCRYPTION AND DECRYPTION

- RSA does not directly operate on strings of bits as in case of symmetric key encryption. It operates on numbers modulo n. Hence, it is necessary to represent the plaintext as a series of numbers less than n.
- Suppose the sender wish to send some text message to someone whose public key is (n, e).
- The sender then represents the plaintext as a series of numbers less than n.
- To encrypt the first plaintext P, which is a number modulo n. The encryption process is simple mathematical step as $C=P^e \bmod n$

- Returning to our Key Generation example with plaintext P = 10, we get ciphertext $C=10^5 \mod 91$
- The decryption process for RSA is also very straightforward. Suppose that the receiver of public-key pair (n, e) has received a ciphertext C. Receiver raises C to the power of his private key d. The result modulo n will be the plaintext P.

$$\text{Plaintext}=C^d \bmod n = 82^{29} \bmod 91 = 10$$

By Narendra Bohara

EXAMPLE 2

1. Select two prime numbers, p=17 and q =11.
2. Calculate $n = pq$ = 17 × 11 = 187.
3. Calculate $\varphi(n)$= (p-1)*(q-1)= 16 × 10=160.
4. Select e such that e is relatively prime to $\varphi(n)$= 160 and less than $\varphi(n)$; we choose e=7.
5. Determine d such that de mod 160=1 and d < 160. The correct value is d=23, because 23 × 7 =161=(1 × 160)+1.
6. For a plaintext input of M = 88,

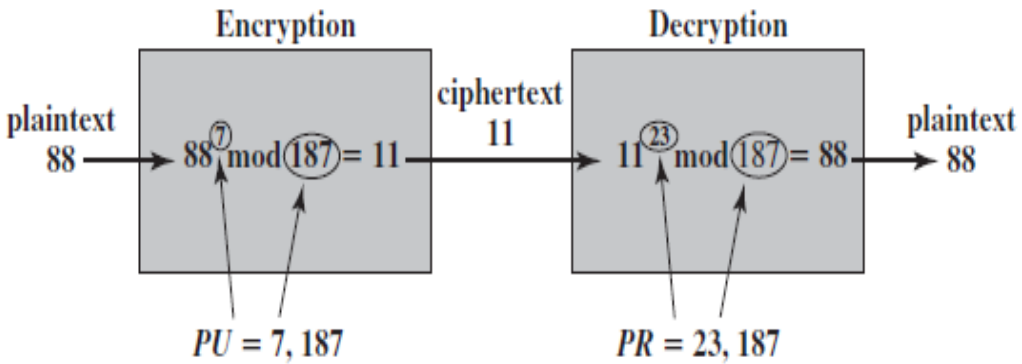


Figure 3.11 Example of RSA Algorithm

By Narendra Bohara

USING THE PROPERTIES OF MODULAR ARITHMETIC FOR SIMPLICITY,

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$
$$88^1 \bmod 187 = 88$$
$$88^2 \bmod 187 = 7744 \bmod 187 = 77$$
$$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$$
$$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$$

For decryption, we calculate $M = 11^{23} \bmod 187$:

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$
$$11^1 \bmod 187 = 11$$
$$11^2 \bmod 187 = 121$$
$$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$$
$$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$$
$$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187$$
$$= 79{,}720{,}245 \bmod 187 = 88$$

By Narendra Bohara

PRIMITIVE ROOT OF A PRIME NUMBER

- A primitive root of a prime number as one whose powers modulo generate all the integers from 1 to p-1 .That is, if is a primitive root of the prime number , then the numbers

$$a \bmod p, a^2 \bmod p, \ldots\ldots, a^{p-1} \bmod p$$

are distinct and consist of the integers from 1 through p-1 in some permutation.

By Narendra Bohara

DIFFIE-HELLMAN KEY-EXCHANGE ALGORITHM

- Diffie-Hellman was the first public-key algorithm, invented, way back in 1976.
- It gets its security from the difficulty of calculating discrete logarithms in a finite field.
- The purpose of the algorithm is to enable two users to securely exchange a key that can then be used for subsequent encryption of messages.
- The algorithm itself is limited to the exchange of secret values.
- i.e. Diffie-Hellman can be used for key distribution—Alice and Bob can use this algorithm to generate a secret key—but it cannot be used to encrypt and decrypt messages.

By Narendra Bohara

DIFFIE-HELLMAN KEY-EXCHANGE ALGORITHM CONTD..

- There are two publicly known numbers: a prime number q and an integer α that is a primitive root of q. Suppose the users A and B wish to exchange a key.
- User A selects a rando m integer $X_A < q$, computes $Y_A = a^{XA} \bmod q$
- Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = a^{XB} \bmod q$.
- Each side keeps the X value private and makes the Y value available publicly to the other side.
- User A computes the key as $K = (Y_B)^{XA} \bmod q$ *and* user B computes the key as $K = (Y_A)^{XB} \bmod q$.
- These two calculations produce identical results??????

- The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithms. For large primes, the latter task is considered infeasible.

By Narendra Bohara

DIAGRAMATIC REPRESENTATION OF **DIFFIE-HELLMAN KEY-EXCHANGE**

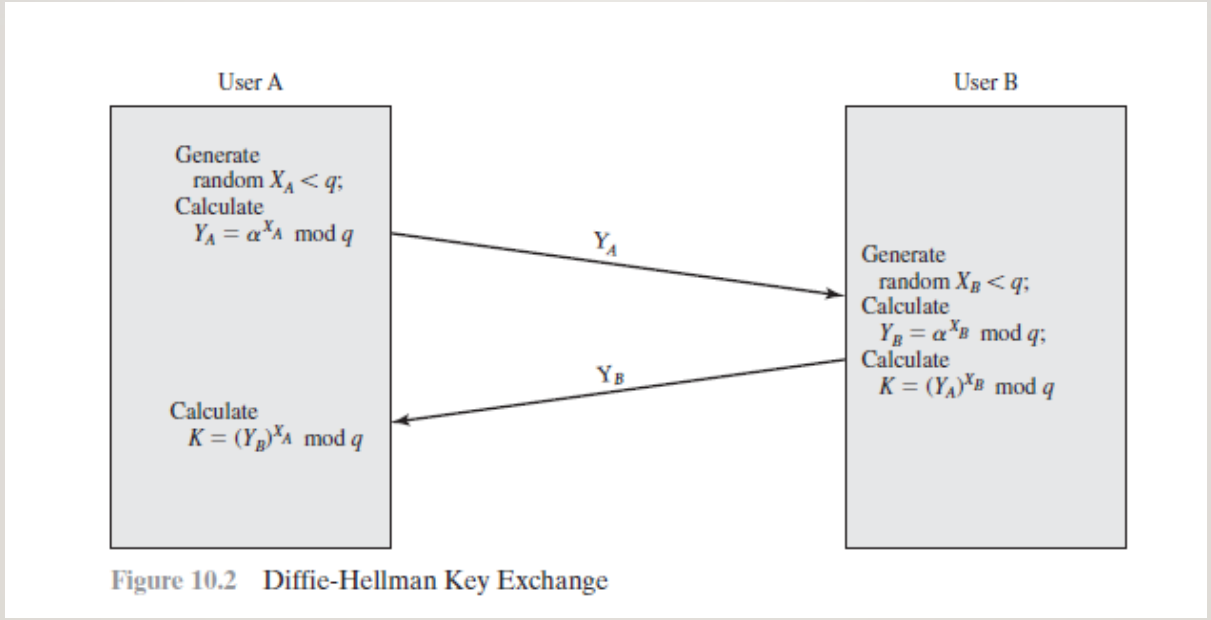


Figure 10.2 Diffie-Hellman Key Exchange

EXAMPLE

- Key exchange is based on the use of the prime number $q = 353$ and a primitive root of 353, in this case a = 3.
- A and B select secret keys $X_A = 97$ and $X_B = 233$, respectively.
- Each computes its public key:
- A computes $Y_A = 3^{97} \bmod 353 = 40$.
- B computes $Y_B = 3^{233} \bmod 353 = 248$.
- After they exchange public keys, each can compute the common secret key:

- A computes $K = (Y_B)^{XA} \bmod 353 = 248^{97} \bmod 353 = 160$.
- B computes $K = (Y_A)^{XB} \bmod 353 = 40^{233} \bmod 353 = 160$.

By Narendra Bohara

MAN-IN-THE-MIDDLE ATTACK

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

1. Darth prepares for the attack by generating two random private keys X_{D1} and X_{D2} and then computing the corresponding public keys Y_{D1} and Y_{D2}.
2. Alice transmits Y_A to Bob.
3. Darth intercepts Y_A and transmits Y_{D1} to Bob. Darth also calculates $K_2 = (Y_A)^{X}{}_{D2} \bmod q$.
4. Bob receives Y_{D1} and calculates $K1 = (Y_{D1})^{XB}$ modq

5. Bob transmits Y_B to Alice.
6. Darth intercepts *YB AND* transmits Y_{D2} to Alice. Darth calculates $K_1 = (Y_B)X_{D1} \bmod q$.
7. Alice receives Y_{D2} and calculates $K_2 = (Y_{D2})^{XA} \bmod q$.

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key K_1 and Alice and Darth share secret key K_2.

All future communication between Bob and Alice is compromised ??

By Narendra Bohara

HOW FUTURE COMMUNICATION BETWEEN BOB AND ALICE IS COMPROMISED??

1. Alice sends an encrypted message M: E($K2$, M) .
2. Darth intercepts the encrypted message and decrypts it to recover M.
3. Darth sends Bob $E(K1, M)$ or E($K1$, 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

By Narendra Bohara

ELGAMAL CRYPTOGRAPHIC SYSTEM

- In 1984, T. Elgamal announced a public-key scheme based on discrete logarithms closely related to the Diffie-Hellman technique.
- ElGamal cryptosystem is used in some form in a number of standards including the digital signature standard (DSS), and the S/MIME ,e-mail standard.

As with Diffie-Hellman, the global elements of ElGamal are a prime number q *and* α which is a primitive root of q. User A generates a private/public key pair as follows:

1. Generate a random integer X_A, such that $1 < X_A < q - 1$.
2. Compute $Y^A = \alpha^{X_A} \bmod q$.
3. A's private key is X_A; A's pubic key is $\{q, \alpha, Y_A\}$.

Any user B that has access to A's public key can encrypt a message as follows:

1. Represent the message as an integer M in the range $0 \leq M \leq q - 1$. Longer messages are sent as a sequence of blocks, with each block being an integer less than q.
2. Choose a random integer k such that $1 \leq k \leq q - 1$.
3. Compute a one-time key $K = (Y_A)^k \bmod q$.
4. Encrypt M as the pair of integers (C_1, C_2) where

$$C_1 = \alpha^k \bmod q; \quad C_2 = KM \bmod q$$

User A recovers the plaintext as follows:

1. Recover the key by computing $K = (C_1)^{X_A} \bmod q$.
2. Compute $M = (C_2 K^{-1}) \bmod q$.

By Narendra Bohara

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:	$M = (C_2 K^{-1}) \bmod q$

Figure 10.3 The ElGamal Cryptosystem

By Narendra Bohara

EXAMPLE

- let us start with the prime field GF(19); that is, q=19. It has primitive roots {2, 3, 10, 13, 14, 15}. We choose **α=10.**
- Alice generates a key pair as follows:

1. Alice chooses X_A=5.
2. $Y_A = \alpha^{XA}{}_{Mod\ q=10}{}^{5}\ Mod\ 19=3.$
3. Alice's private key is 5;Alice's pubic key is $\{q, \alpha, Y_A\}$ = {19, 10, 3}.

Suppose Bob wants to send the message with the value M=17.Then

1. Bob chooses k=6.
2. Then **K**= $(Y_A)^k$ *mod q= 3^6mod19=729mod19=7.*
3. *Now* C_1= α^K**modq=10^6mod19=11.**

   C_2= ***K****M* mod q=7*17Mod 19=119Mod19=5.
4. Bob sends the ciphertext (11, 5).

By Narendra Bohara

FOR DECRYPTION

1. Alice calculates $K = (C_1)^{XA} \ mod \ q = 11^5 \ mod \ 19 = 161051 \bmod 19 = 7$.
2. Then K^{-1} in GF(19) is $7^{-1} \bmod 19 = 11$ (use extended Euclidean algorithm).
3. Finally $M = (C2K^{-1}) \bmod q = 5 * 11 \bmod 19 = 55 \bmod 19 = 17$.

By Narendra Bohara

TASKS

- Analyze Security part of **ELGAMAL CRYPTOGRAPHIC SYSTEM. In which parameters its security depend and how secure is the ELGAMAL CRYPTOGRAPHIC SYSTEM?**
- Miller-Rabin Algorithm for Primality Testing.