Chapter 3 – Asymmetric Key Cryptography

- By

Jyoti Tryambake

Public Key Cryptosystems (1)

- Public-key/two-key/asymmetric cryptography involves the use of two keys: –
  - a public-key, which may be known by anybody, and can be used to encrypt messages, and verify signatures
  - a related private-key, known only to the recipient, used to decrypt messages, and sign (create) signatures
- Is asymmetric because – those who encrypt messages or verify signatures cannot decrypt messages or create signatures
- 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.

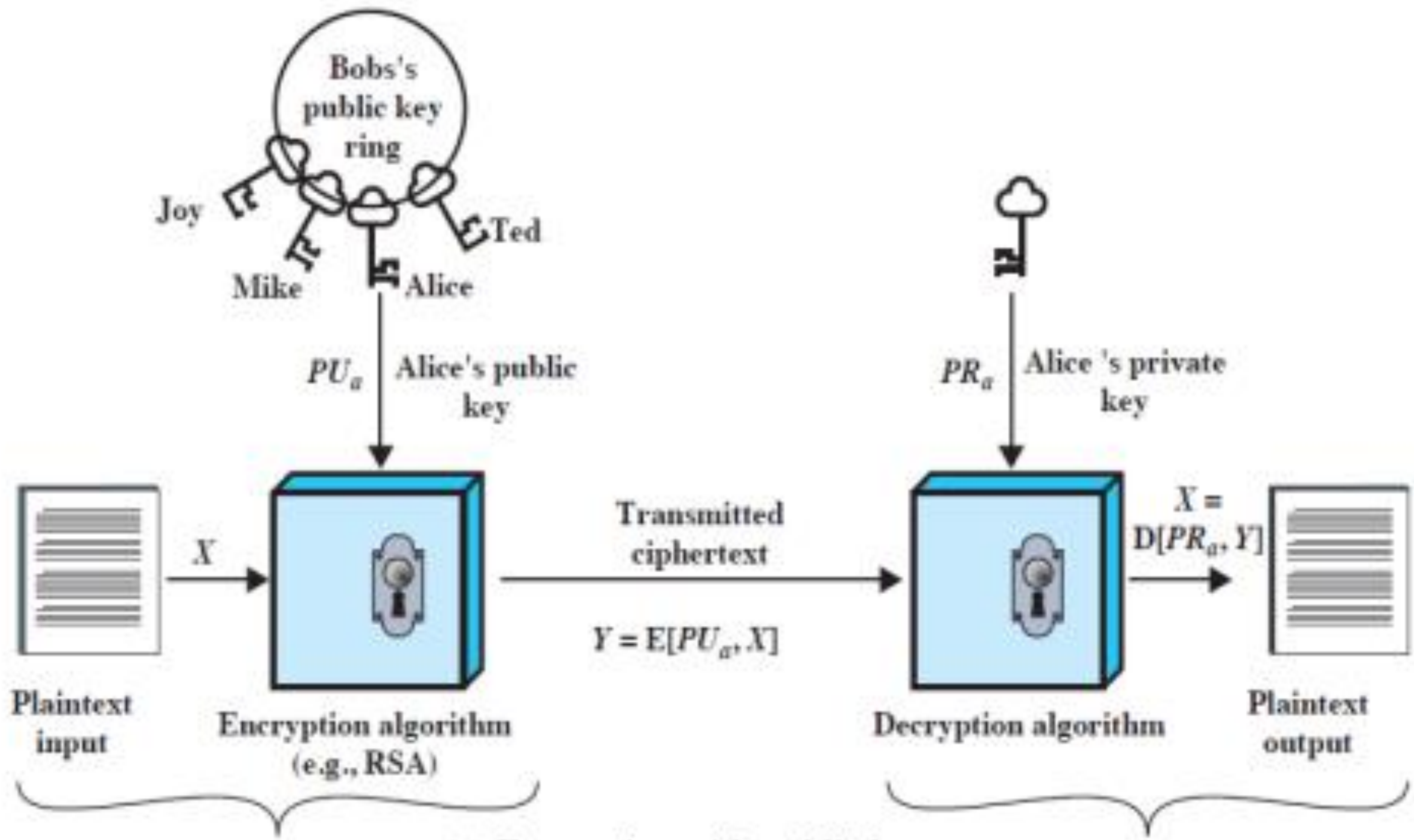
Public-Key Cryptosystems (2)

- 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.
  - A public-key encryption scheme has following ingredients
    - **Plaintext**: This is the readable message or data that is fed into the algorithm as input.
    - **Encryption algorithm**: The encryption algorithm performs various transformations on the plaintext.
    - **Public and private keys**: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
    - **Decryption algorithm:** This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Terms for further slides ..

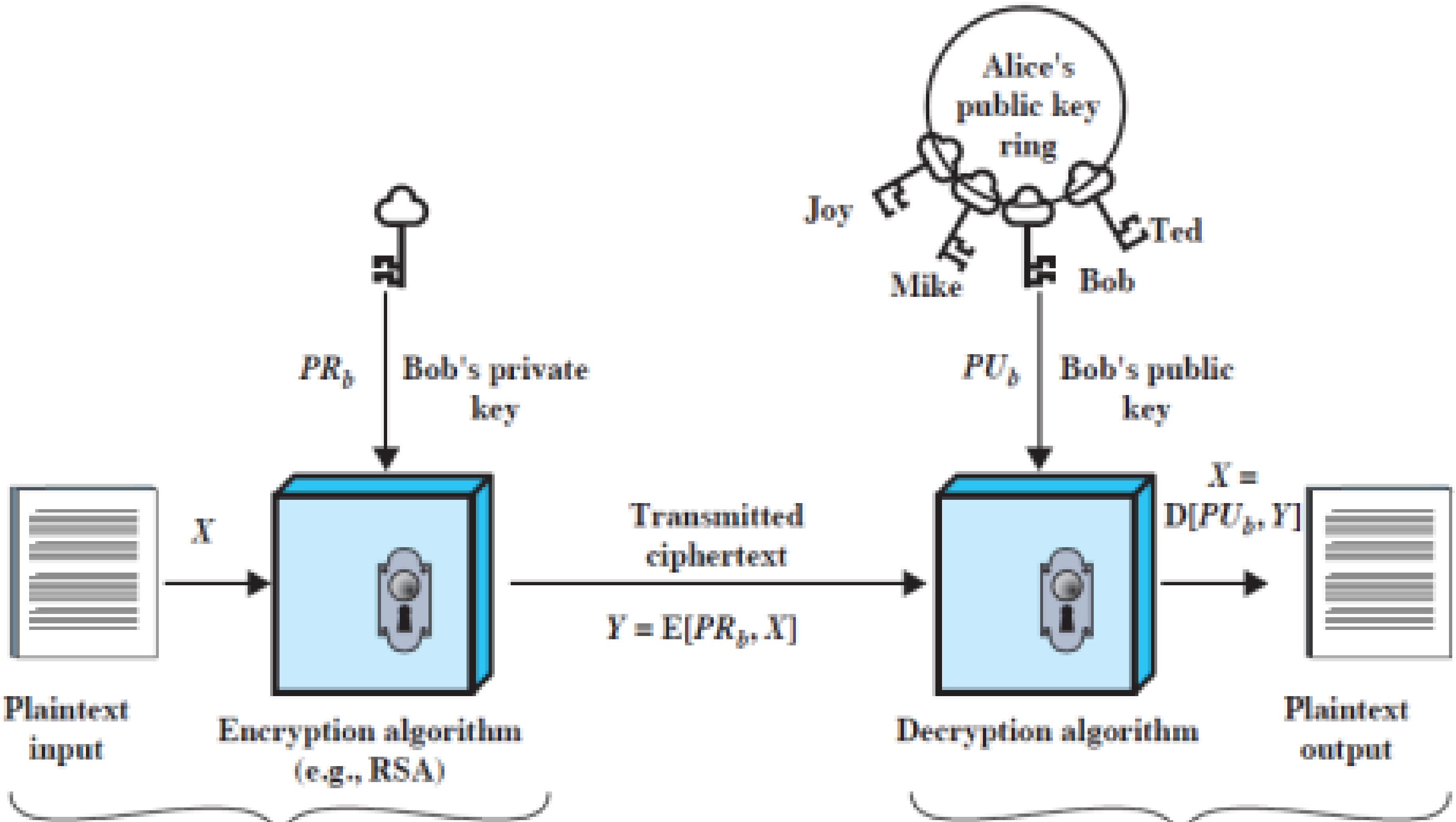
- There is some source A that produces a message in plaintext, $X = [X_1, X_2, ..., X_M]$.
- The M elements of X are letters in some finite alphabet.
- The message is intended for destination B.
- B generates a related pair of keys: a public key, PU_b, and a private key, PR_b.
- PR_b is known only to B, whereas PU_b is publicly available and therefore accessible by A.
- With the message X and the encryption key PU_b as input, A forms the ciphertext $Y = [Y_1, Y_2, ... , Y_N]$:
    - $Y = E(PU_b, X)$
  - The intended receiver, in possession of the matching private key, is able to invert the transformation:
    - $X = D(PR_b, Y)$

Public Key Cryptosystems (3)



(a) Encryption with public key

Public Key Cryptosystems (4)

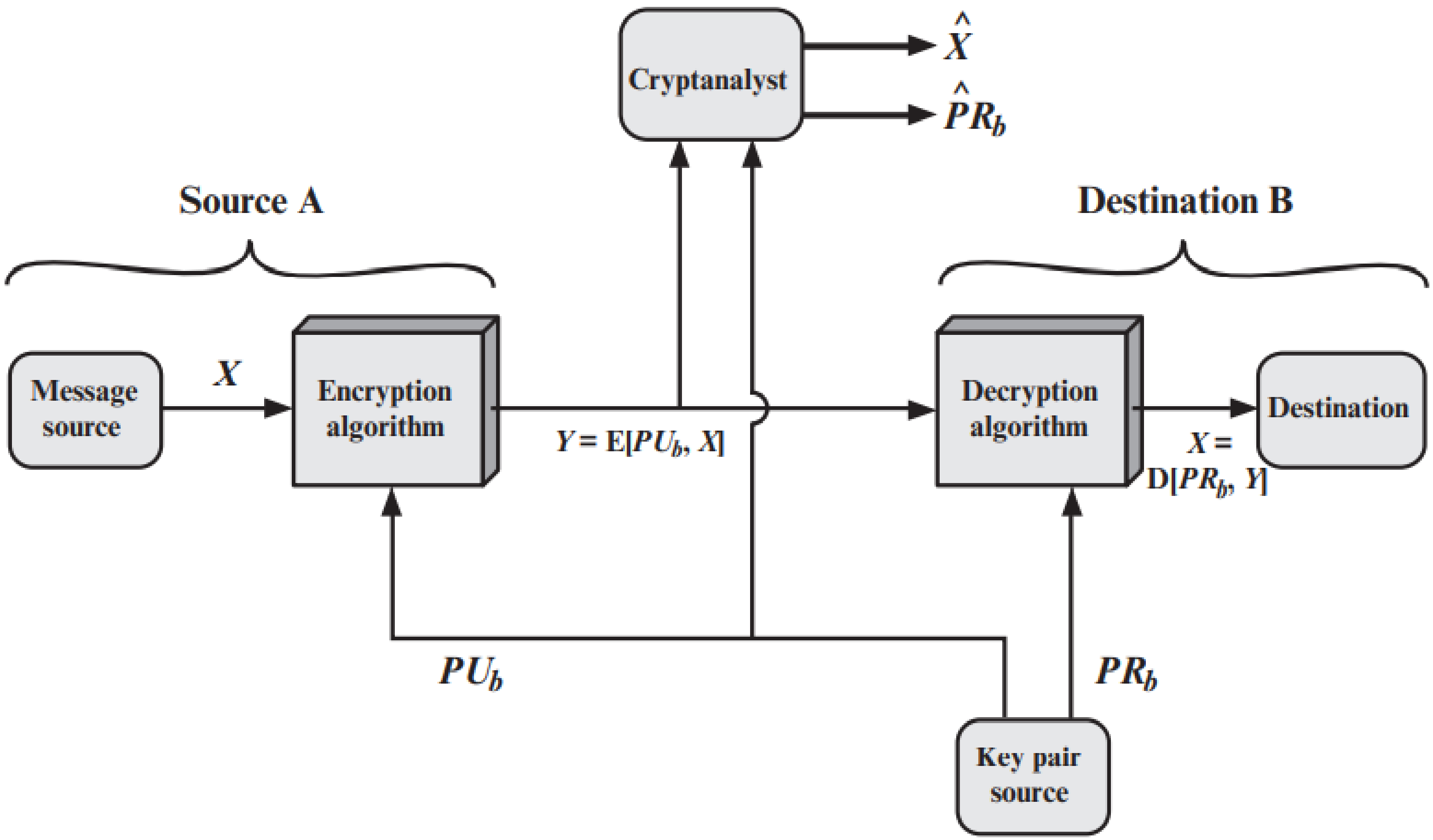


(b) Encryption with private key

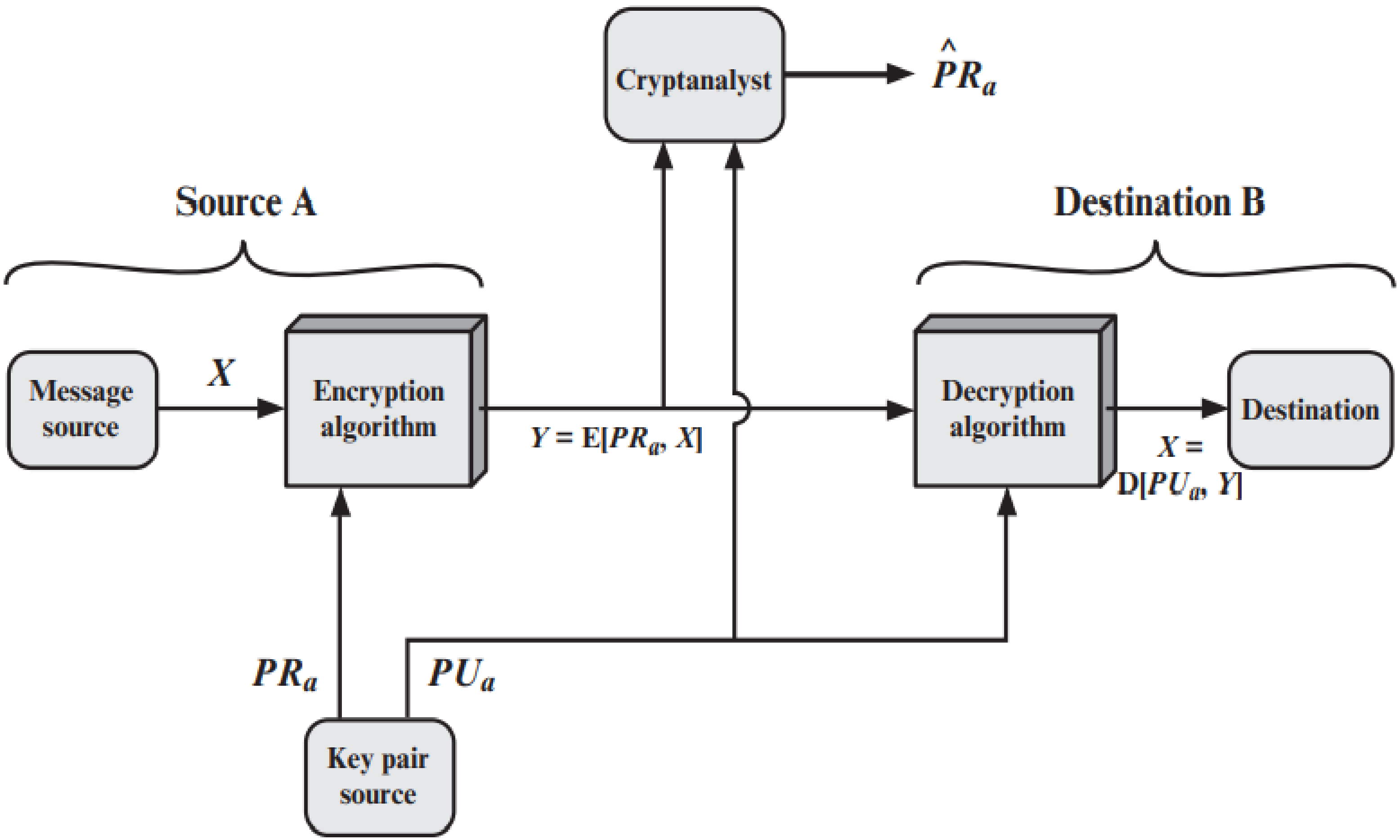
Table 9.2 Conventional and Public-Key Encryption

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.

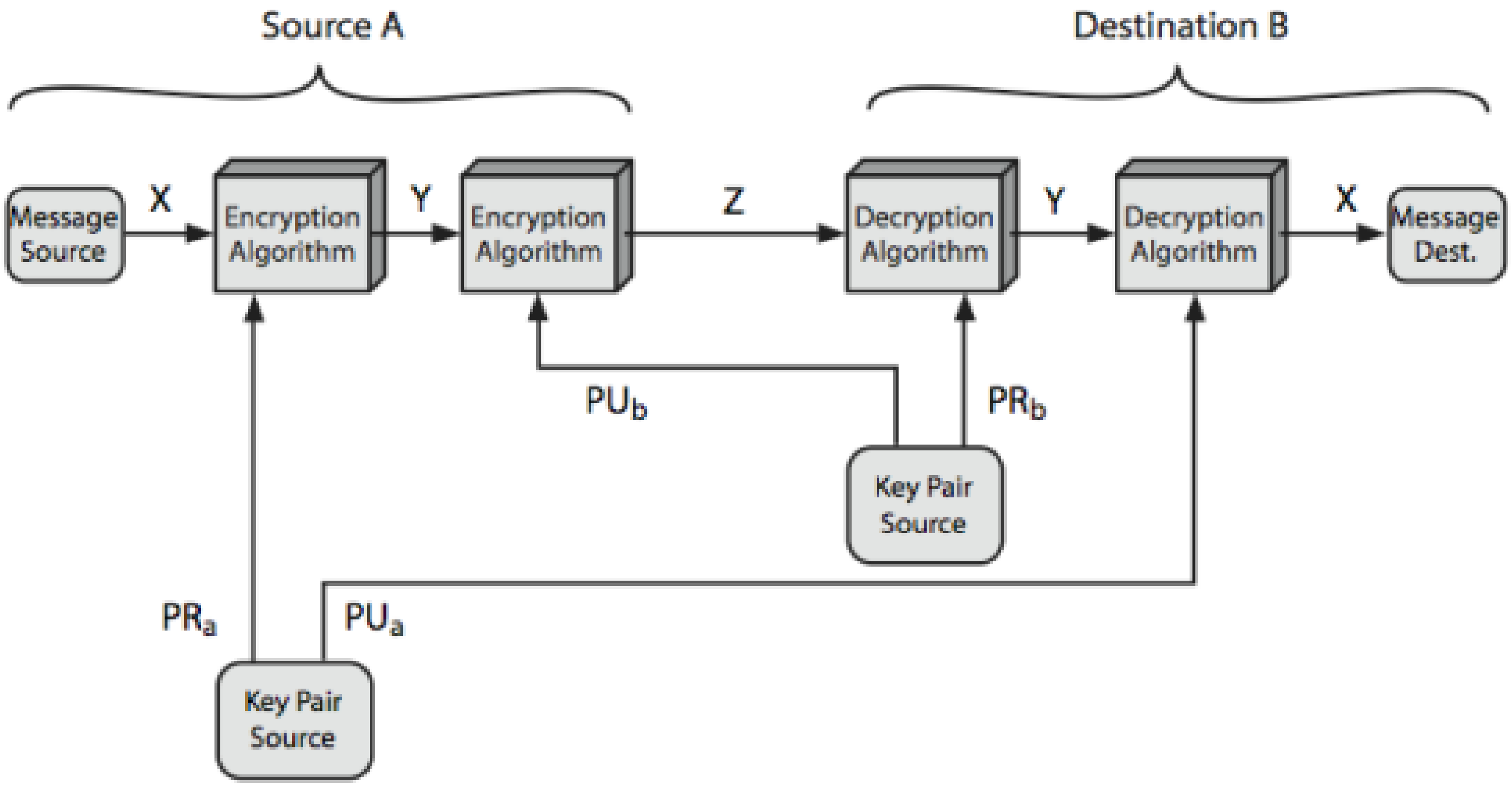
Public Key Cryptosystems - Confidentiality



Public Key Cryptosystems - Authentication



Public Key Cryptosystems



Combining secrecy and authentication

Application of public key cryptography

- **Encryption/Decryption**: sender encrypts the message with receiver's public key
- **Digital Signature** : sender signs the message with his private key
- **Key exchange**: Both sender and receiver cooperate to exchange a session key typically for conventional encryption.

Application of public key cryptography

Table 9.3 Applications for Public-Key Cryptosystems

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

Requirements of Public Key Cryptography (1)

Algorithm must fulfill;

- It is computationally easy for a party B to generate a key pair (public key PU_b, private key PR_b).
- It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext:
  - $C = E(PU_b, M)$
- It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:
  - $M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$

Requirements of Public Key Cryptography (2)

Algorithm must fulfill;

- It is computationally infeasible for an adversary, knowing the public key, PU_b, to determine the private key, $PR_{b.}$
- It is computationally infeasible for an adversary, knowing the public key, PU_b, and a ciphertext C, to recover the original message, M.
- The two keys can be applied in either order:
  - $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$

The RSA Algorithm (1)

- It was developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT and first published in 1978 [RIVE78].
- The Rivest-Shamir-Adleman (RSA) scheme has since that time reigned supreme as the most widely accepted and implemented general-purpose approach to public-key encryption.
- The **RSA** scheme is a cipher in which the plaintext and ciphertext are integers between 0 and $n - 1$ for some n.
- A typical size for n is 1024 bits, n is less than 2^{1024}.

The RSA Algorithm (2)

Description

- RSA makes use of an expression with exponentials.
- Plaintext is encrypted in blocks, with each block having a binary value less than some number *n*. That is, the block size must be less than or equal to $\log_2(n) + 1$;
- in practice, the block size is *i* bits, where $2^i < n <= 2^{i+1}$
- Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C.
  - $C = M^e \bmod n$
  - $M = C^d \bmod n$

The RSA Algorithm (3)

Description

- Both sender and receiver must know the value of n.
- The sender knows the value of e, and only the receiver knows the value of d.
- Thus, this is a public key encryption algorithm with

a public key of $PU = \{e, n\}$ and

a private key of $PR = \{d, n\}$.

The RSA Algorithm (4)

Description

- For this algorithm to be satisfactory for public-key encryption, the following requirements must be met.

1. It is possible to find values of e, d, n such that $M^{ed} \bmod n = M$ for all $M < n$.
2. It is relatively easy to calculate $M^e \bmod n$ and $C^d \bmod n$ for all values of $M < n$.
3. It is infeasible to determine d given e and n.

The RSA Algorithm (5)

The preceding relationship holds if e and d are multiplicative inverses modulo $\phi(n)$, where $\phi(n)$ is the Euler totient function. It is shown in Appendix B that for p, q prime, $\phi(pq) = (p - 1)(q - 1)$. $\phi(n)$, referred to as the Euler totient of n, is the number of positive integers less than n and relatively prime to n. The relationship between e and d can be expressed as

$$ed \bmod \phi(n) = 1$$

This is equivalent to saying

$$ed \bmod \phi(n) = 1$$
$$d \bmod \phi(n) = e^{-1}$$

That is, e and d are multiplicative inverses mod $\phi(n)$. According to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to $\phi(n)$. Equivalently, $\gcd(\phi(n),d) = 1$; that is, the greatest common divisor of $\phi(n)$ and d is 1.

The RSA Algorithm (5)

Figure 21.5 summarizes the RSA algorithm. Begin by selecting two prime numbers, p and q, and calculating their product n, which is the modulus for encryption and decryption. Next, we need the quantity $\phi(n)$. Then select an integer e that is relatively prime to $\phi(n)$ [i.e., the greatest common divisor of e and $\phi(n)$ is 1]. Finally, calculate d as the multiplicative inverse of e, modulo $\phi(n)$. It can be shown that d and e have the desired properties.

RSA Scheme

Key Generation by 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:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

RSA Numerical

Example 1

- P=3, q=5
- N = p*q =15
- Φ(n) = (p-1)(q-1) = 2*4 = 8
- Gcd(e, Φ(n)) = 1 where, 1<e< Φ(n)
- Let e = 3

de mod Φ(n) = 1

d * 3 mod 8 = 1

- So, d = 3
- Public key = (e,n) = (3,15)
- Private key = (d,n) = (3,15)
- Let M= 4
  - $C = M^e \bmod n = 4^3 \bmod 15 = 4$
  - $M = C^d \bmod n = 4^3 \bmod 15 = \mathbf{4}$

Key Generation by 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:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

RSA Numerical

Example 2

- P=11, q=3

Key Generation by 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:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

RSA Numerical

Example 2

- P=11, q=3
- N = p*q =33
- Φ(n) = (p-1)(q-1) = 10*2 = 20
- Gcd(e, Φ(n)) = 1 where, 1<e< Φ(n)
- Let e = 3

de mod Φ(n) = 1

d * 3 mod 20 = 1

- So, d = 7
- Public key = (e,n) = (3,33)
- Private key = (d,n) = (7,33)
- Let M= 7
  - $C = M^e \bmod n = 7^3 \bmod 33 = 13$
  - $M = C^d \bmod n = 13^7 \bmod 33 =$ **7**

Key Generation by 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:	$M = C^d \bmod n$

Figure 9.5 The RSA Algorithm

Attacks on RSA

Attacks on RSA

- Mathematical attack
  - Factorization
  - Common Modulus
- Short Message attack
- Timing attack
- Cycling attack
- Chosen cipher attack

Factorization attacks on RSA

- Factoring is splitting an integer into a set of smaller integers which, when multiplied together form the original integer.
- The problem: for example, 2*7 = 14 .
- The factoring problem is to find 2 and 7 when given 14. Prime factorization requires splitting an integer into factors that are prime numbers.
- This problem in factoring that an RSA modulus would allow an attacker to figure out the private key from the public key.

Factorization attacks on RSA (cont.)

- The solution: choose two large primes with a larger modulus for becoming a larger and so, the attacker needs more time to figure it out.

- Tow primes should be one is much smaller than other.

- If the two primes are extremely close or their difference is close to any predetermined amount, then there is a potential security risk, but the probability that two randomly chosen primes are so close is negligible.

Common Modulus Attack

❖ If multiple entities share the same modulus $n=pq$ with different pairs of (e_i, d_i), it is not secure. Do not share the same modulus!

❖ Cryptanalysis: If the same message M was encrypted to different users

User u_1 : $C_1 = M^{e_1} \bmod n$

User u_2 : $C_2 = M^{e_2} \bmod n$

If $\gcd(e_1, e_2)=1$, there are a and b s.t. $ae_1 + be_2 = 1 \bmod n$

Then,

$$(C_1)^a(C_2)^b \bmod n = (M^{e_1})^a(M^{e_2})^b \bmod n = M^{ae_1+be_2} \bmod n = M \bmod n$$

Short Message Attack

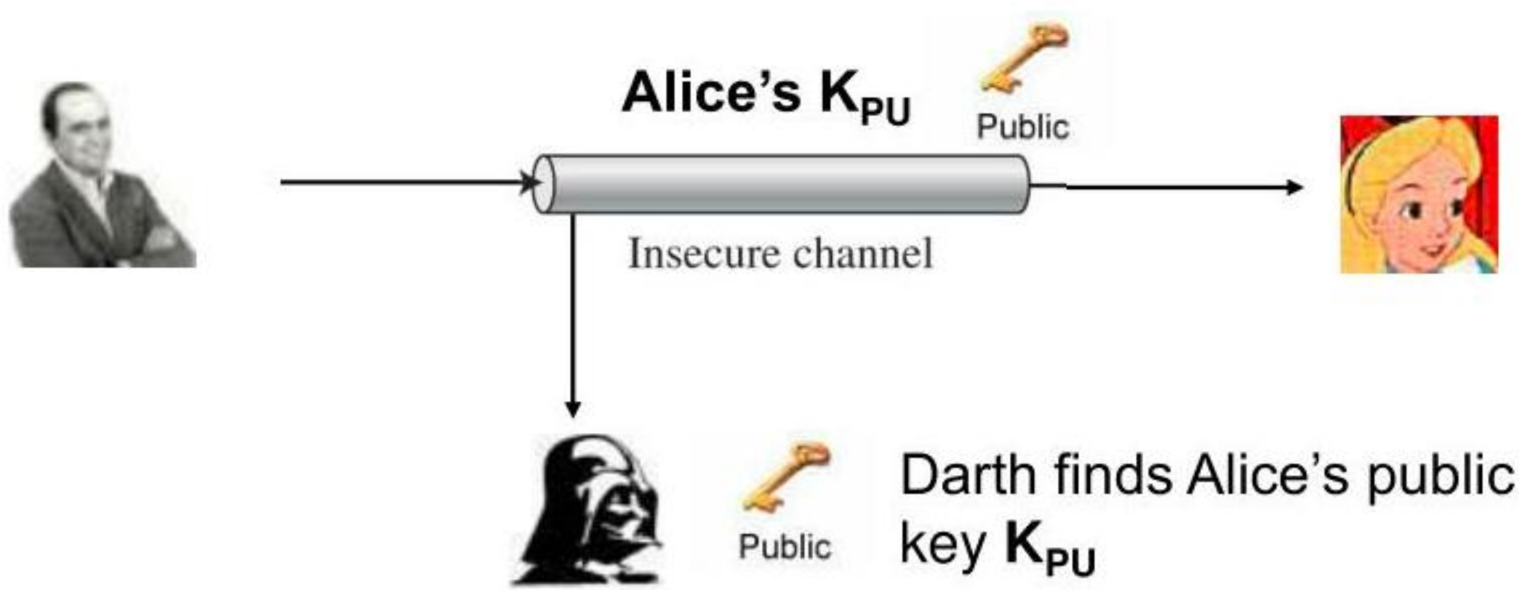
- Typical use of public key algorithm:
  Generating short messages
  - Symmetric keys (used then to send rest of message)
  - Social security numbers, etc.

- Idea:
  - Adversary acquires public key ***E***, ***n***
  - Uses them to encrypt all possible messages that may be sent (plausible if messages are short enough!) and stores in table
  - Intercepts encrypted message ***C*** and searches for match in the table

Adversary can recover plaintext without decryption key!

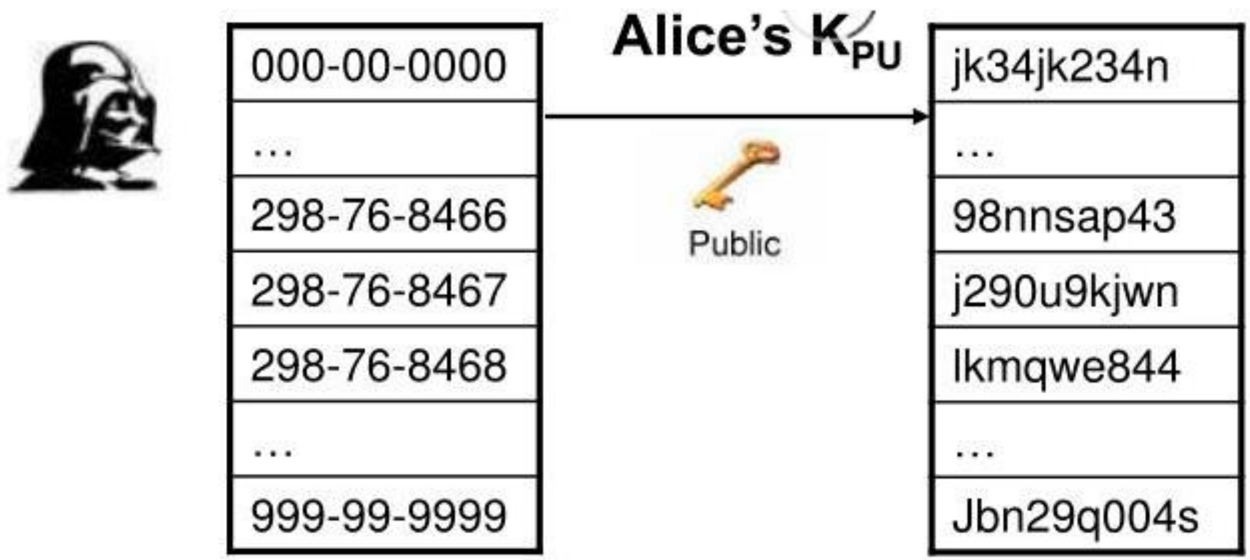
Short Message Attack (cont.)

- Example:
  Darth knows that Bob will use Alice's public key to send her a <u>Social Security Number</u> (9 digits)



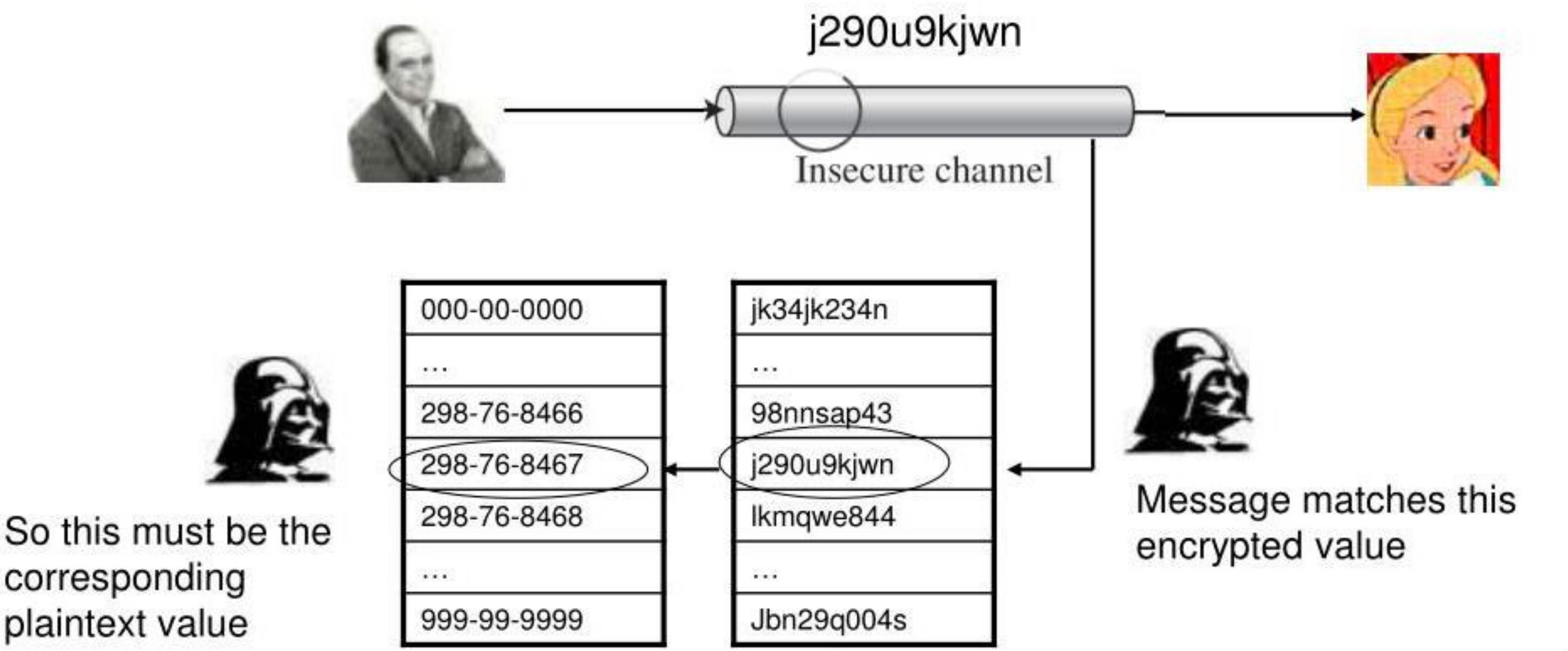
Short Message Attack (cont.)

- Darth uses Alice's public key $\mathbf{K_{PU}}$ to encrypt <u>all possible Social Security Numbers</u>
  (only a billion)



Short Message Attack (cont.)

- Darth intercepts Bob's SSN encrypted with Alice's public key
- Searches for <u>match</u> in table of encrypted values



Short Message Attack (cont.)

- Solution: Pad message to ***M*** bits
  - ***M*** large enough so adversary can't generate all $\mathbf{2}^{M}$ possible messages
  - Can't just add extra bits to end – still possible to crack

- Optimal Asymmetric Encryption Padding (OAEP)
  - Additional bits used as "mask" to conceal plaintext
    - Mask generated randomly
    - Mask data sent as part of encrypted message for decryption
  - Based on cryptographic hash (more later)

Timing Attack

- If adversary knows the following:
  - Ciphertext ***C***
    - Can be intercepted
    - Can compute how long it takes to multiply ciphertext and compute mods
  - Total time decryption takes
    - Can be observed

  They could compute number of 1's in private ***D***

- Given enough known plaintexts, can reliably guess ***D*** completely

Timing Attack (cont.)

- Fast exponentiation algorithm used for decryption to compute C^D mod n:

```
result = 1
for (i = 0 to number of bits in D - 1) {
   if (i^th bit of D = 1)
      result = (result * C) mod n
   C = C^2 mod n
   }
```

- Speed of decryption depends on number of **1**'s in ***D***
  - Each **1** requires additional multiplication operation
  - Each **0** skips that step

Timing Attack (cont.)

Solutions:

- "Pad" algorithm so all decryptions take same time

```
for (i = 0 to number of bits in D - 1) {
  if (ith bit of D = 1) result = (result * C) mod n
  else garbageVariable = (result * C) mod n
  C = C2 mod n
  }
```

Cycling Attack

Cycling Attack

Since $c = m^e \bmod n$, encryption maps message m to one of the elements of the message space $Z_n = \{0, 1, \ldots, n-1\}$. If the encryption is applied repeatedly on c, eventually a stage[7] will arrive when c will get mapped to m. The adversary uses this fact to his advantage. He intercepts a ciphertext c, he carries out repeat encryptions of c till he gets back the intercepted ciphertext c. He goes back by one step because the message encrypted last must be the original plaintext m. It has been shown that computational complexity of this attack is equivalent to the complexity of factoring n.

Example 2 Bob sends ciphertext 37 to Alice after using her RSA public key $\{7, 77\}$. The adversary intercepts the ciphertext and launches cycling attack using the public key of Alice. Write the computation carried out by the adversary to decrypt the ciphertext.

Solution The adversary encrypts 37 repeatedly as given below:

$c_1 = 37^7 \bmod 77 = 16$

$c_2 = 16^7 \bmod 77 = 58$

$c_3 = 58^7 \bmod 77 = 9$

$c_4 = 9^7 \bmod 77 = 37$

In the fourth step he gets $c_4 = 37$. Therefore, he concludes Bob's message is 9.

Unconcealed Messages

An unconcealed message is one that encrypts to itself, i.e., $c = m^e \bmod n = m$. For example, messages $0, 1, n-1$ always remain unconcealed. The number of unconcealed messages in Z_n is given by

$$[1 + \gcd(e-1, p-1)] \times [1 + \gcd(e-1, q-1)]$$

Chosen Cipher Attack

Chosen-Ciphertext Attack

This attack is based on multiplicative property of RSA algorithm. Let m_1 and m_2 be two messages, and let c_1 and c_2 be their respective RSA encryptions. Now,

$$(m_1 m_2)^e \bmod n = m_1^e m_2^e \bmod n = (m_1^e \bmod n) \times (m_2^e \bmod n) = c_1 c_2$$

In other words, RSA encryption of product of two messages is the product of their respective encryptions. The adversary can use this property to decrypt illegitimately copied ciphertext. Suppose Bob sends to Alice a ciphertext c, which the adversary copies. We assume that Alice will decrypt arbitrary ciphertext from the adversary other than c. The adversary conceals c in c' as $c' = cx^e \bmod n$, where x is a random integer in Z_n^* and has multiplicative inverse in Z_n^*. He sends c' to Alice for decryption. Alice computes m' and returns it to the adversary.

$$m' = (c')^d \bmod n = (cx^e)^d \bmod n = c^d x^{ed} \bmod n = mx \bmod n$$

The adversary computes m by multiplying m' and multiplicative inverse of x.

$$m' \, x^{-1} \bmod n = m \, x \, x^{-1} \bmod n = m$$

This simple attack can be prevented by imposing a structure to the plaintext m, e.g. by appending a pad to m. Alice would notice structural discrepancy of m' when she decrypts c', and she would not return the decrypted message m' to the adversary. The process of appending a pad to plaintext for this purpose is sometimes known as 'salting' the plaintext.

Reference : https://crypto.stackexchange.com/questions/2323/how-does-a-chosen-plaintext-attack-on-rsa-work

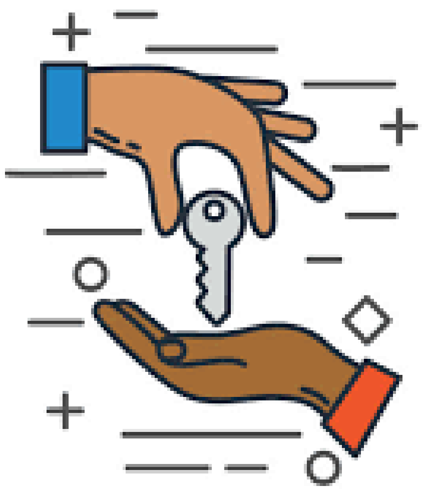
Elliptic Curve Cryptography

- ECC can be defined as: EC over Z_p and EC over $GF(2^m)$.
- ECC can be used for Key exchange and Encryption.

Elliptic curves over Z_p :

- The curve of this type is **prime curve**
- The variables and coefficients are restricted to elements of a finite field.
- The values are restricted from 0 through p-1. If the values exceeds the range perform modulo p.
- The curve is represented by $y^2 \bmod p = (x^3 + ax + b) \bmod p$

How can two people in a crowded room derive a secret that only the pair know, without revealing the secret to anyone else that might be listening?



Diffie Hellman Key Exchange(1)

- The **Diffie-Hellman Key Exchange is a means for two parties to jointly establish a shared secret over an unsecure channel**, without having any prior knowledge of each other.
- This protocol is widely used in protocols like IPSec and SSL/TLS.
- Using this protocol, sending and receiving devices in a network derive a secret key then be used for subsequent symmetric encryption of messages.

Diffie Hellman Key Exchange(2)

- Not an encryption algo
- Used to exchange secret key between two users
- Uses asymmetric encryption to exchange the secret key
- Depends for its effectiveness on the difficulty of computing Discrete Logarithms (Refer Chapter – Number Theory (Stalling)).

Diffie Hellman Key Exchange(3)

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

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

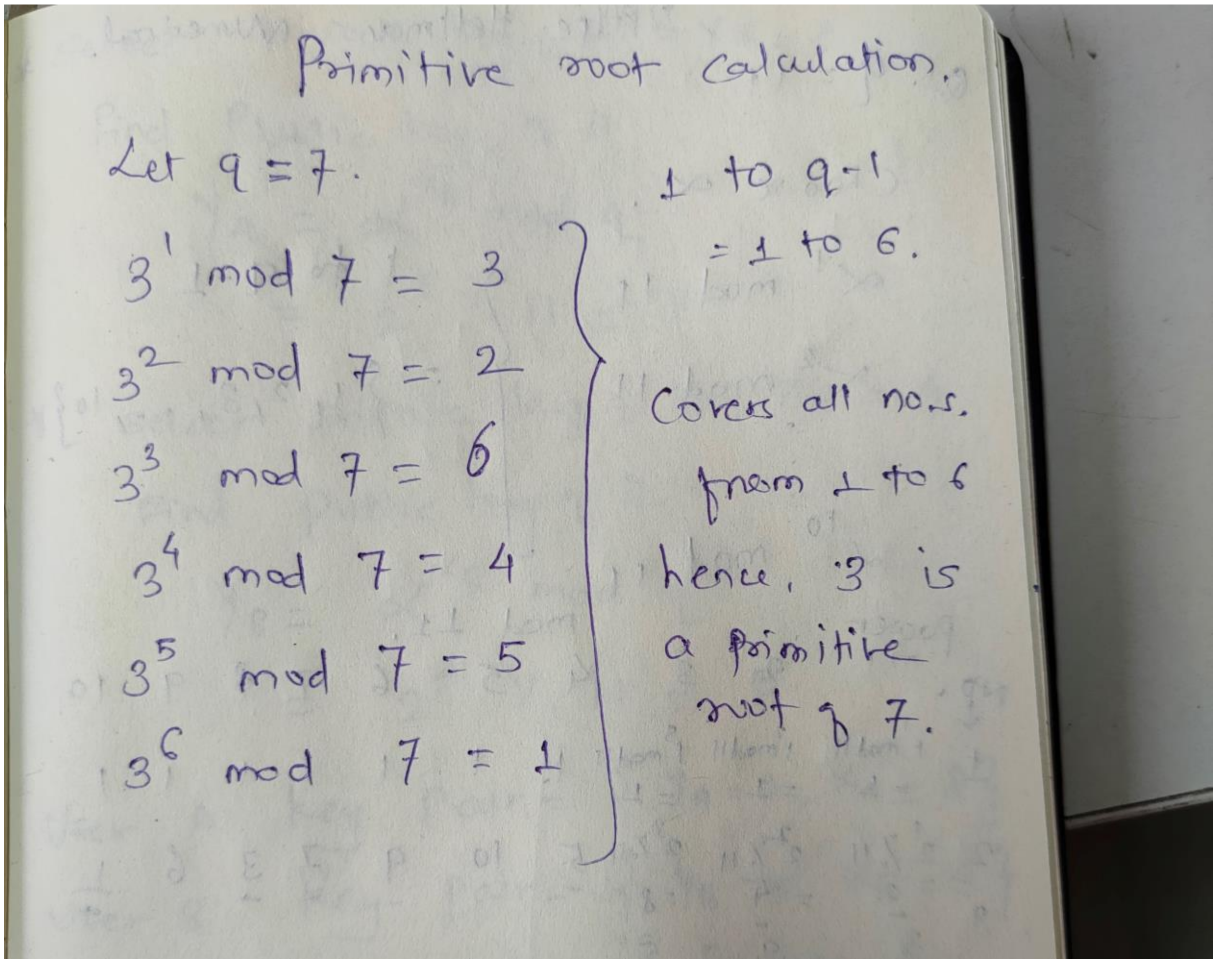
are distinct and consist of the integers from 1 through $p - 1$ in some permutation.

For any integer b and a primitive root a of prime number p, we can find a unique exponent i such that

$$b \equiv a^i \pmod{p} \qquad \text{where } 0 \leq i \leq (p-1)$$

- The exponent i is referred to as the discrete logarithm of b for the base a, mod p expressed as $\mathrm{dlog}_{a,p}(b)$.

Primitive root example



Primitive root calculation.

Let $q = 7$.

$3^1 \bmod 7 = 3$

$3^2 \bmod 7 = 2$

$3^3 \bmod 7 = 6$

$3^4 \bmod 7 = 4$

$3^5 \bmod 7 = 5$

$3^6 \bmod 7 = 1$

1 to $q-1$

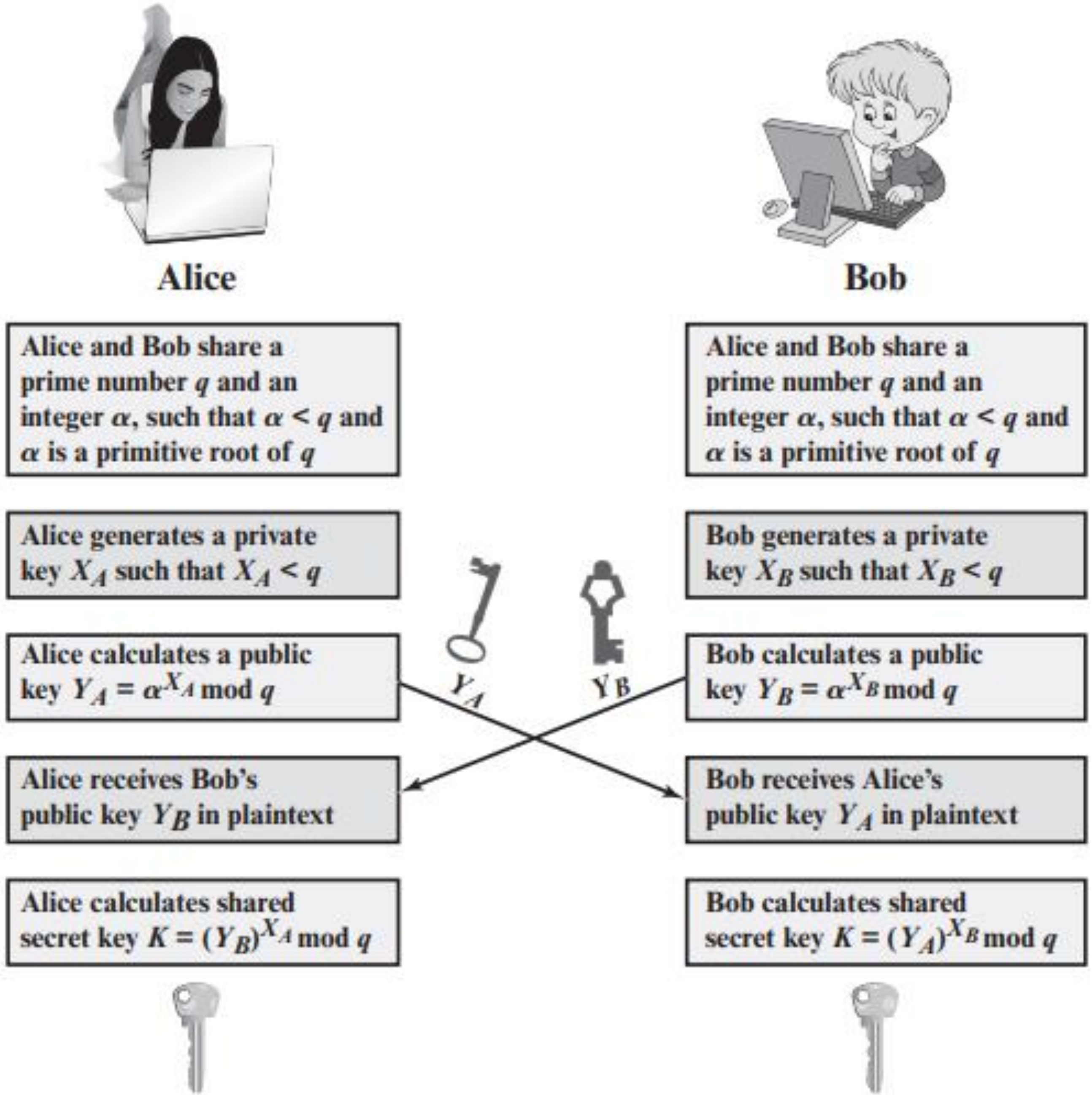
$= 1$ to 6.

Covers all no.s. from 1 to 6

hence, 3 is a primitive root of 7.

DH Algorithm Key terms…

- Twp publicly known numbers:
  - A prime number q
  - An integer α = primitive root of q
- User A
  - Random integer X_A (private key of A) < q
    - Compute Y_A (public key of A) = $\alpha^{X_A} \bmod q$
    - Compute $K = (Y_B)^{X_A} \bmod q$
- User B
  - Random integer X_B (private key of B) < q
    - Compute Y_B (public key of B) = $\alpha^{X_B} \bmod q$
    - Compute $K = (Y_A)^{X_B} \bmod q$
- K should be identical


Alice
Bob
Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q
Alice and Bob share a prime number q and an integer α, such that $\alpha < q$ and α is a primitive root of q
Alice generates a private key X_A such that $X_A < q$
Bob generates a private key X_B such that $X_B < q$
Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$
Y_A
Y_B
Bob calculates a public key $Y_B = \alpha^{X_B} \bmod q$
Alice receives Bob's public key Y_B in plaintext
Bob receives Alice's public key Y_A in plaintext
Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$
Bob calculates shared secret key $K = (Y_A)^{X_B} \bmod q$

DH Numerical

Example 1

Let q = 11,

Find primitive root α ,

We get α = 2

Q1. $q = 11$

Choose α.

1 to $q-1$

$\alpha^1 \bmod 11$

$\alpha^2 \bmod 11$

⋮

$\alpha^{10} \bmod 11$

$= \{1, 2, 3, \ldots, 10\}$

mod 11.

No. ↓ / power →	1	2	3	4	5	6	7	8	9	10
1	$1^1 \bmod 11 = 1$	$1^2 \bmod 11 = 1$	$1^3 \bmod 11 = 1$	1	1	1	1	1	1	1
2	$2^1 \% 11 = 2$	$2^2 \% 11 = 4$	$2^3 \% 11 = 8$	5	10	9	7	3	6	1
3	3	9	5							
4										
5										
6										
7										
8										
9										
10										

So $\alpha = 2$, as it is Primitive root of

DH Numerical

Example 1 (cont.)

Select $X_A = 8$

- Compute Y_A (public key of A) = $\alpha^{X_A} \bmod q = 2^8 \bmod 11 = 3$

Select $X_B = 4$

- Compute Y_B (public key of B) = $\alpha^{X_B} \bmod q = 2^4 \bmod 11 = 5$

Sender A -> Computes $K = (Y_B)^{X_A} \bmod q = 5^8 \bmod 11 = 4$

Sender B -> Computes $K = (Y_A)^{X_B} \bmod q = 3^4 \bmod 11 = 4$

DH Numerical

Example 2

In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?

Ans - 16

Security Aspect of DH

Possibility to compute Private key and preventive measures

- Let q = 353 , α = 3, Y_A = 40 and Y_B = 248

- Prevention – choose large primary key

Man in the Middle Attack

- Allows attacker to eavesdrop on the communication between two users. Attack takes place during exchange of public keys.

Analogy: 2 users- Alice and bob, Attacker- Darth

- Darth could tell Alice that he was bob and tell bob that she was Alice
- Alice would believe and reveal her conversation to Darth.
- Darth gathers information, alters and pass the message to Bob.
- Thus, conversation is hijacked.

Man in the Middle Attack – Scenario (1)

- Select X_{D1} and X_{D2}
- $Y_{D1} = \alpha^{X_{D1}} \mod q$
- $Y_{D2} = \alpha^{X_{D2}} \mod q$

DARTH

- Select X_A
- $Y_A = \alpha^{X_A} \mod q$

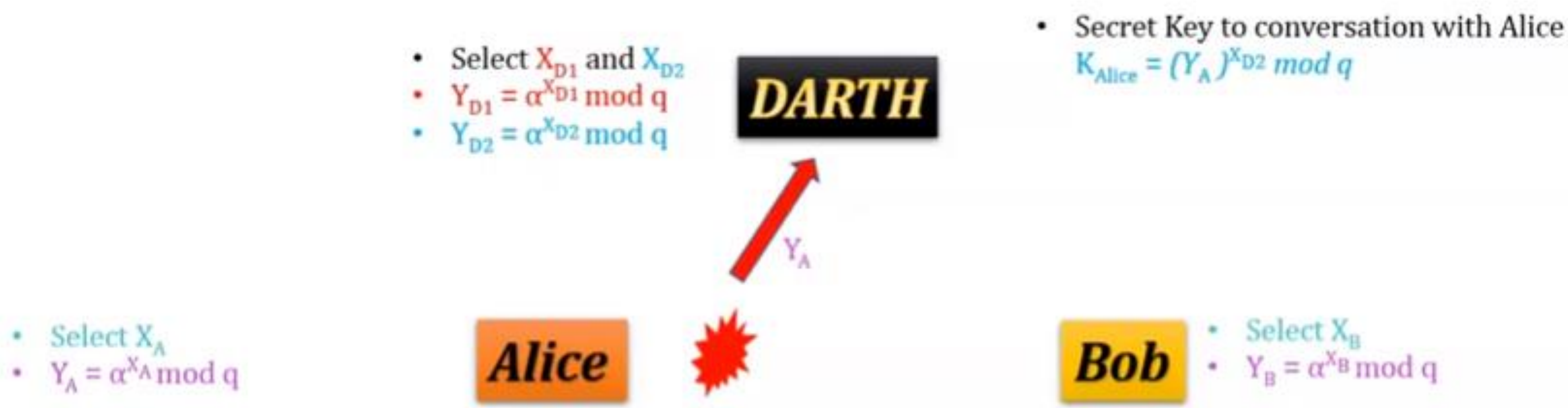
Alice

Bob

- Select X_B
- $Y_B = \alpha^{X_B} \mod q$

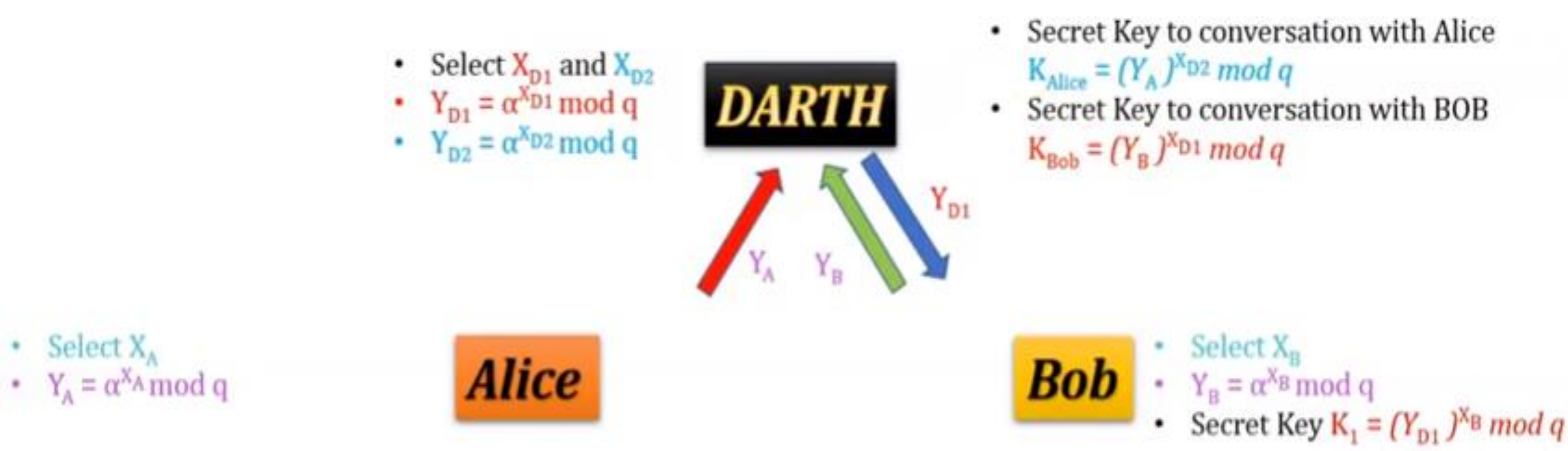
- *Darth prepares for the attack,*
  - Generating two random private keys X_{D1} and X_{D2}
  - Calculate public key Y_{D1}
  - Calculate public key Y_{D2}

Man in the Middle Attack – Scenario (2)



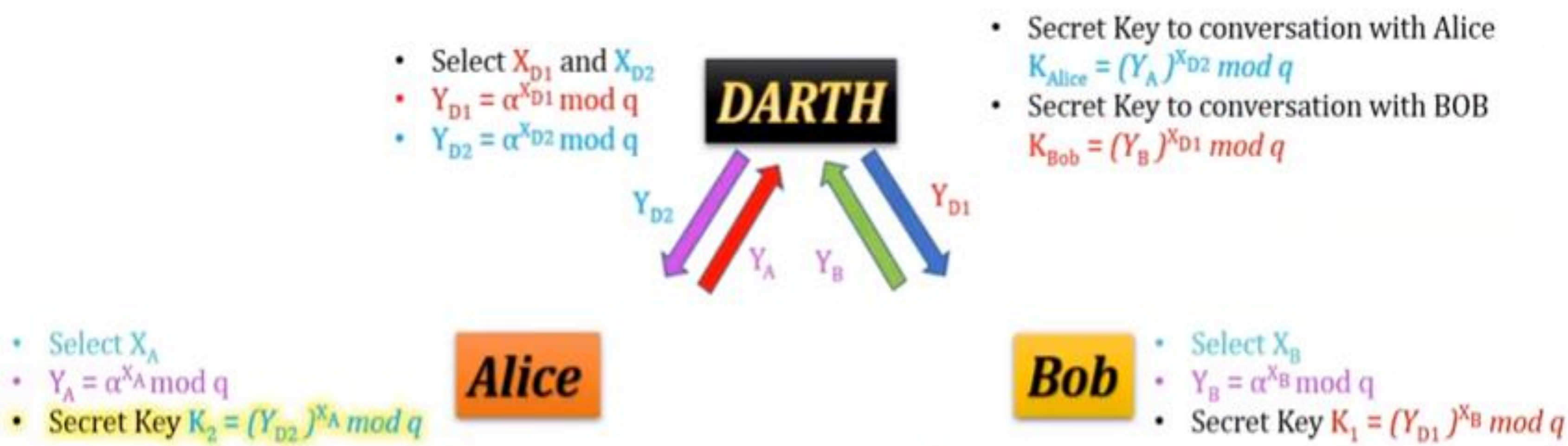
- As per key exchange algorithm, Alice transmits her public key Y_A to Bob.
- Darth intercepts Y_A
- Darth calculate secret key K_{Alice} for more conversation with Alice. $K_{Alice} = (Y_A)^{X_{D2}} \bmod q$.

Man in the Middle Attack – Scenario (3)



- Darth transmits Y_{D1} (in place of Y_A)to Bob. Bob doesn't have an idea, Y_{D1} is shared by Darth.
- Bob calculate secret key K_1 using Y_{D1}. Secret Key $K_1 = (Y_{D1})^{X_B} \bmod q$.
- *Bob* transmits his public key Y_B to Alice.
- Darth intercepts Y_B.
- Darth calculate secret key K_{Bob} for more conversation with Bob. $K_{Bob} = (Y_B)^{X_{D1}} \bmod q$

Man in the Middle Attack – Scenario (4)



- Darth transmits Y_{D2} (in place of Y_B)to Alice. Alice doesn't have an idea, Y_{D2} is shared by Darth.
- Alice calculate secret key K_2 using Y_{D2}. Secret Key $K_2 = (Y_{D2})^{X_A} \bmod q$.
- Now, Darth will capture all subsequent messages of Alice and Bob. Read and modify all the message and send to the alice and Bob.

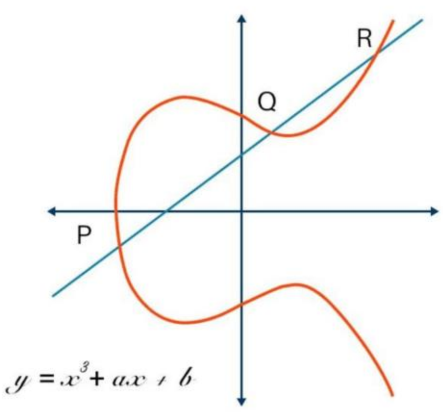
This vulnerability can be overcome with the use of digital signatures and public-key certificates;

Elliptic Curve Cryptography

- Asymmetric /public key cryptosystem
- Provides equal security with smaller key size
- Reduces processing overhead
- Makes use of elliptic curves
- Defined by some mathematical functions:
  - $y^2 = x^3 + ax + b$
  - Elliptic curve is represented as Ep(a,b).

  P is a prime number and a,b are restricted

  to mod p.



Elliptic Curves over Real Numbers

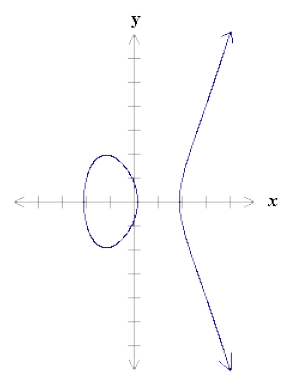
Elliptic curves over real numbers use a special class of elliptic curves of the form

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

In the above equation, if $4a^3 + 27b^2 \neq 0$, the equation represents a **nonsingular elliptic curve;** otherwise, the equation represented a **singular elliptic curve.**

where x, y, a and b are real numbers.

Each choice of the numbers a and b yields a different elliptic curve. For example, a = -4 and b = 0.67 gives the elliptic curve with equation $y^2 = x^3 - 4x + 0.67$; the graph of this curve is shown below:



$y^2 = x^3 - 4x + 0.67$

Elliptic Curves over Real Numbers

Elliptic curves over real numbers use a special class of elliptic curves of the form

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

In the above equation, if $4a^3 + 27b^2 \neq 0$, the equation represents a **nonsingular elliptic curve;** otherwise, the equation represented a **singular elliptic curve.**

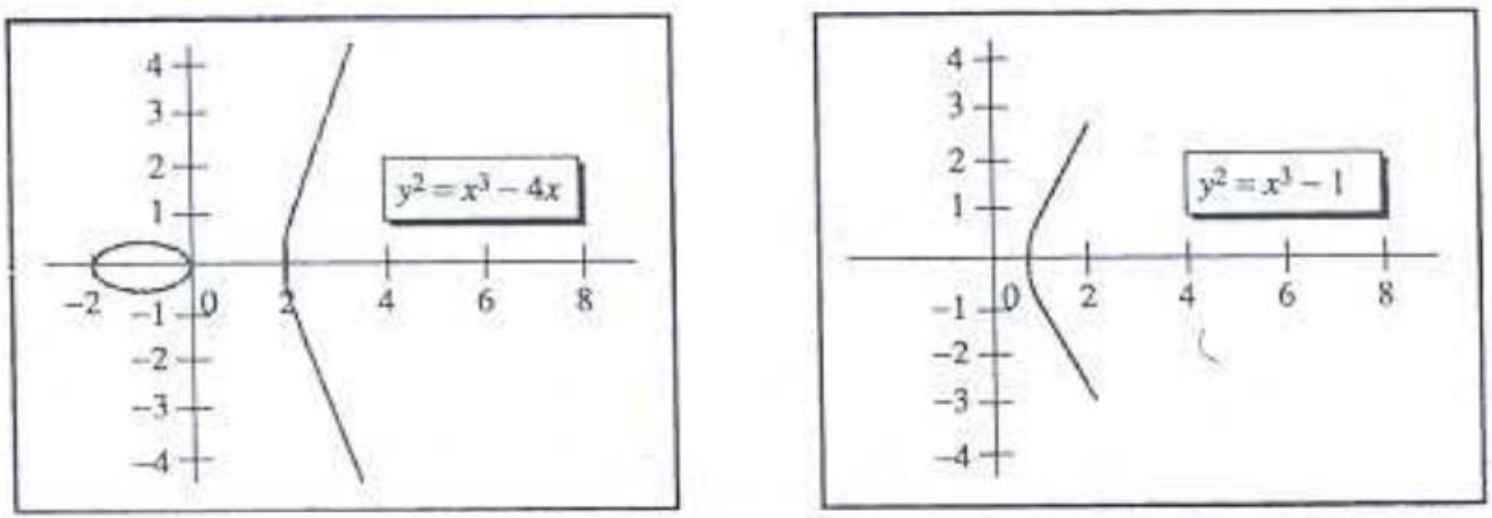
Looking at the equation, we can see that the left-hand side has a degree of 2 while the right-hand side has a degree of 3. This means that a horizontal line can intersects the curve in three points if all roots are real. However, a vertical line can intersects the curve at most in two points.

Elliptic Curves over Real Numbers

Example 10.13

Figure 10.12 shows two elliptic curves with equations $y^2 = x^3 - 4x$ and $y^2 = x^3 - 1$. Both are non-singular. However, the first has three real roots ($x = -2$, $x = 0$, and $x = 2$), but the second has only one real root ($x = 1$) and two imaginary ones.

Figure 10.12 *Two elliptic curves over a real field*



a. Three real roots

b. One real and two imaginary roots

Elliptic Curve Cryptography

- Abelian groups:- commutative group

Operations

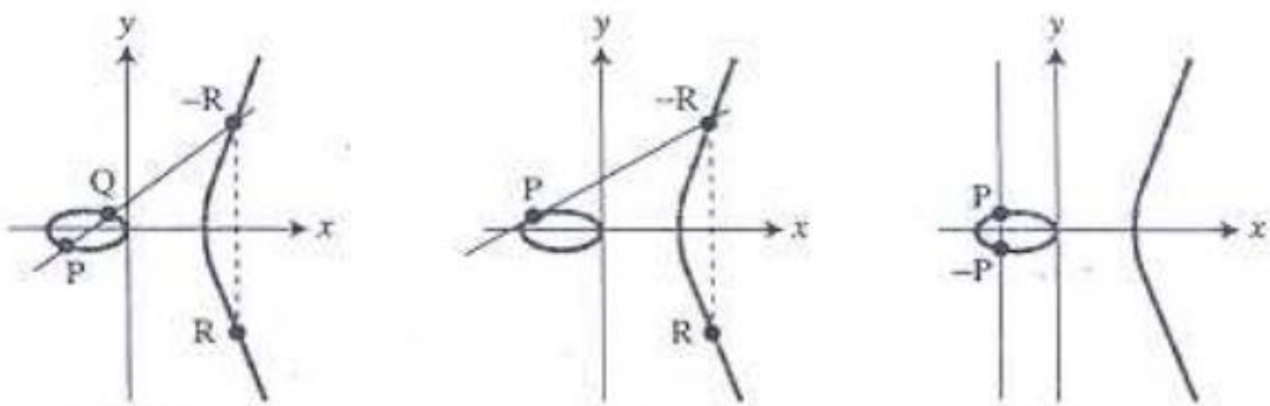
ECC- Addition operation on the points of curve

. The operation is the addition of two points on the curve to get another point on the curve

$$R = P + Q, \text{ where } P = (x_1, y_1),\ Q = (x_2, y_2), \text{ and } R = (x_3, y_3)$$

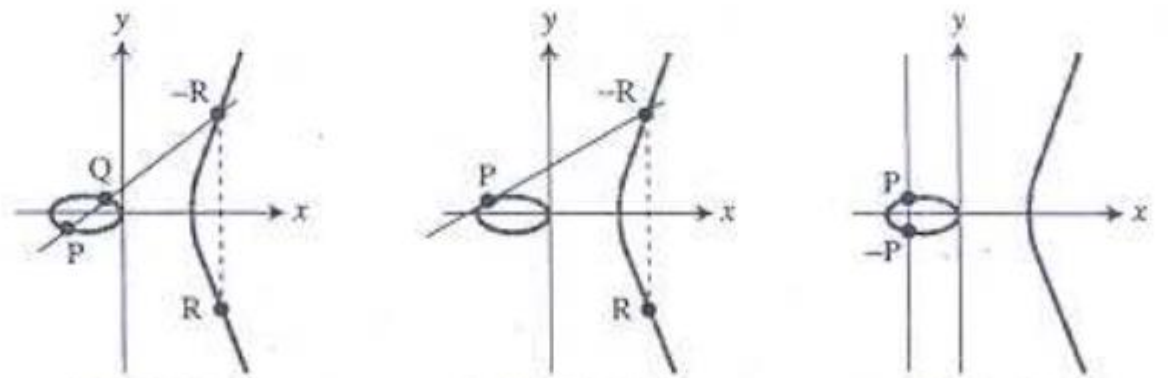
To find R on the curve, consider three cases as shown in Figure 10.13.

Figure 10.13 *Three adding cases in an elliptic curve*



a. (R = P + Q) b. (R = P + P) c. (O = P + (– P))

ECC- Addition operation on the points of curve (cont.)



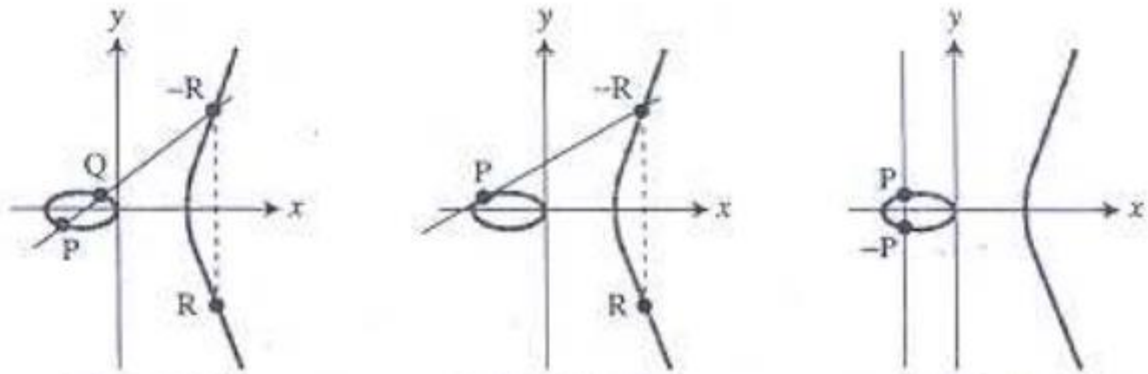
a. (R = P + Q) b. (R = P + P) c. (O = P + (– P))

1. In the first case, the two points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ have different x-coordinates and y-coordinates ($x_1 \neq y_1$ and $x_2 \neq y_2$), as shown in Figure 10.13a. The line connecting P and Q intercepts the curve at a point called –R. R is the reflection of –R with respect to the x-axis. The coordinates of the point R, x_3 and y_3, can be found by first finding the slope of the line, λ, and then calculating the values of x_3 and y_3, as shown below:

$$\lambda = (y_2 - y_1) / (x_2 - x_1)$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda\,(x_1 - x_3) - y_1$$

ECC- Addition operation on the points of curve (cont.)



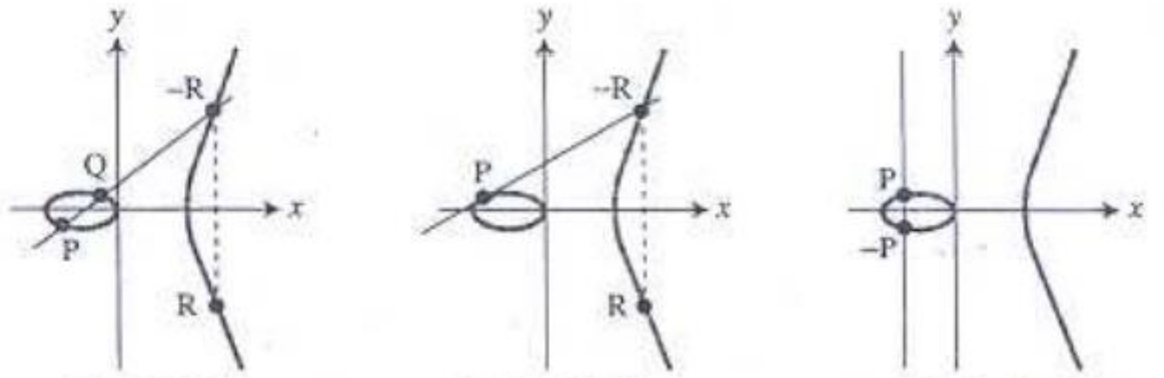
a. (R = P + Q) b. (R = P + P) c. (O = P + (– P))

2. In the second case, the two points overlap (R = P + P), as shown in Figure 10.13b. In this case, the slope of the line and the coordinates of the point R can be found as shown below:

$$\lambda = (3x_1^2 + a)/(2y_1)$$

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

ECC- Addition operation on the points of curve (cont.)



a. (R = P + Q)   b. (R = P + P)   c. (O = P + (– P))

3. In the third case, the two points are additive inverses of each other as shown in Figure 10.13c. If the first point is P = (x_1, y_1), the second point is Q = $(x_1, -y_1)$. The line connecting the two points does not intercept the curve at a third point. Mathematicians say that the intercepting point is at infinity; they define a point $\boldsymbol{O}$ as the *point at infinity* or *zero point*, which is the *additive identity* of the group.

ECC- Addition operation on the points of curve (cont.)

- Abelian groups:

Properties of operation:

  - Closure
  - Associativity
  - Identity element
  - Inverse element
  - Commutativity

ECC- properties of operation

- **Closure:** For all *a*, *b* in *A*, the result of the operation $a \bullet b$ is also in *A*.
- **Associativity:** For all *a*, *b* and *c* in *A*, the equation

  $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ holds.
- **Identity element:** There exists an element *e* in *A*, such that for all elements *a* in *A*, the equation $e \bullet a = a \bullet e = a$ holds.
- **Inverse element:** For each *a* in *A*, there exists an element *b* in *A* such that $a \bullet b = b \bullet a = e$, where *e* is the identity element.
- **Commutativity:** For all *a*, *b* in *A*, $a \bullet b = b \bullet a$.
- A group in which the group operation is not commutative is called a "non-abelian group" or "non-commutative group".

ECC- properties of operation w.r.t. P,Q and R

1. *Closure:* It can be proven that adding two points, using the addition operation defined in the previous section, creates another point on the curve.
2. *Associativity:* It can be proven that $(P + Q) + R = P + (Q + R)$.
3. *Commutativity:* The group made from the points on a non-singular elliptic curve is an abelian group; it can be proven that $P + Q = Q + P$.
4. *Existence of identity:* The additive identity in this case is the *zero point*, O. In other words $P = P + O = O + P$.
5. *Existence of inverse:* Each point on the curve has an inverse. The inverse of a point is its reflection with respect to the x-axis. In other words, the point $P = (x_1, y_1)$ and $Q = (x_1, -y_1)$ are inverses of each other, which means that $P + Q = O$. Note that the identity element is the inverse of itself.

A Group and a Field

The group defines the set of the points on the elliptic curve and the addition operation on the points. The field defines the addition, subtraction, multiplication, and division using operations on real numbers that are needed to find the addition of the points in the group.

ECC over Galois Field GF(p) – modular arithmetic

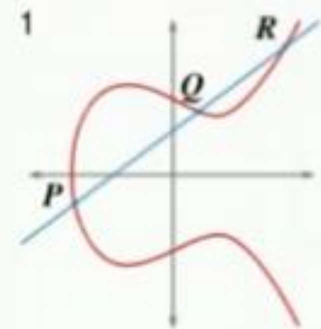
- Same addition operation as that of real numbers but calculations are done in modulo p.

Elliptic curves over Z_p :

- The curve of this type is **prime curve**
- The variables and coefficients are restricted to elements of a finite field.
- The values are restricted from 0 through p-1. If the values exceeds the range perform modulo p.
- The curve is represented by $y^2 \bmod p = (x^3 + ax + b) \bmod p$

ECC over GF(p) – modular arithmetic (cont.)

Elliptic curve arithmetic over Z_p :



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

Addition:

- Adding 2 points $P(x_p, y_p)$ and $Q(x_q, y_q)$ gives $R(x_r, y_r)$.
- Steps:
- **Find the slope λ:**
- $\lambda = (y_q - y_p) / (x_q - x_p)$ if $P \neq Q$
- $\lambda = (3x_p^2 + a) / 2y_p$ if $P = Q$ where a is obtained from $E_p(a,b)$
- Find the Sum: R (i.e (x_r, y_r)) = P + Q
- $x_r = \lambda^2 - x_p - x_q$
- $y_r = \lambda(x_p - x_r) - y_p$

ECC over GF(p) – modular arithmetic (cont.)

Negating a point:

- If $Q = (x_q, y_q)$
- Then $-Q = -(x_q, y_q) = (x_q, -y_q)$

Subtraction: P – Q can be P + (-Q).

- $P - Q = (x_p, y_p) - (x_q, y_q) = (x_p, y_p) + (x_q, -y_q \text{ mod } p)$. Now perform addition.

Multiplication:

- Only Scalar multiplication is possible. Multiplication between two points are not possible. Repeated addition is performed.
- 2P = P + P, 3P = P + P + P and so on. Note for slope (λ) calculation use the formula P=Q.

Division: only scalar division is possible. $[1/a(x_p, y_p)] = a^{-1}(x_p, y_p)$. Multiplication steps can be followed.

ECC over GF(p) – Finding points on curve

$E_{11}(1,6)$ – Given elliptic curve.

$a=1$, $b=6$.

Operating in mod 11 = p.

$y^2 \bmod 11 = x^3+ax+b \pmod{11}$

as per values,

$y^2 = x^2 + x + 6 \pmod{11}$

no.s = 0 ... p-1 = 0 ... 10.

Values of x & y can be from 0 to 10.

Find x and y such that, LHS = RHS and when it satisfies, that point lie on the elliptic curve.

Find x.

x	$x^3+x+6 \pmod{11}$
0	6 % 11 = 6
1	8 % 11 = 8
2	16 % 11 = 5
3	27+3+6 = 36 % 11 = 3
4	8
5	4
6	8
7	4
8	9
9	7
10	4

Find y

y	$y^2 \pmod{11}$
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Find Matching points.

1. $x=2$, $y=4$ and $y=7$. So, (2,4) and (2,7)
2. $x=3$, $y=5$ & $y=6$ (3,5) and (3,6).
3. $x=5$, $y=2$ and $y=9$ (5,2) and (5,9)
4. $x=7$; $y=2$ and $y=9$ (7,2) and (7,9)
5. $x=8$, $y=8$ and $y=3$ (8,3) (8,8)
6. $x=10$, $y=4$ and $y=2$ (10,2) and (10,4)

- For determining the security of various elliptic curve ciphers, it is of some interest to know the number of points in a finite abelian group defined over an elliptic curve.
- In the case of the finite group $E_P(a, b)$, the number of points N is bounded by

$$p + 1 - 2\sqrt{p} \leq N \leq p + 1 + 2\sqrt{p}$$

- Note that the number of points in $E_p(a, b)$ is approximately equal to the number of elements in Z_p, namely p elements.

Understand- find mod for –ve no.

Find mod for -ve no.

Formula, $-n \bmod k = k - (n \bmod k)$

ex i. $-3 \bmod 12$

n — -3, k — 12

$= 12 - (3 \bmod 12) = 12 - 3 = 9$

ii. $-7 \bmod 12$.

$= 12 - (7 \bmod 12)$

$= 12 - (7) = 5$.

iii. $-13 \bmod 12$

$= 12 - (13 \bmod 12)$

$= 12 - (1) = 11$.

iv. $-34 \bmod 23$.

$= 23 - (34 \bmod 23)$

$= 23 - 11 = 12$

Shortcut:

i. $-3 \bmod 12$, $n = 3$, $k = 12$

if $n < k$. i.e. $3 < 12$

then simply subtract n from k

$k - n = 12 - 3 = 9$.

$-7 \bmod 12$, $n < k$.

$k - n = 12 - 7 = 5$.

ii. if $n > k$. i.e. $-34 \bmod 23$

then take multiple of k which should be greater than 'n' & then subtract n from that multiple.

So, $23 \times 1 = 23$, < 34 not applicable

$23 \times 2 = 46$, > 34 ✓

$46 - 34 = 12$ ✓

multiple of 23 — 46, 'n' — 34.

$\therefore -34 \bmod 23 = 12$

OR divide $-34/23 = -11$ ~~$-34 + 23 = -11$~~ and add modulus (23) to make it non-negative, $-11 + 23 = \boxed{12}$

Understand- find mod for –ve no.

$-164 \bmod 23$.

$23 \times 7 = 161 < 164$ ×

$23 \times 8 = 184 > 164$

$\therefore 184 - 164 = 20$.

$-164 \% 23 = 20$.

OR $-164 \% 23 = -3$

$-3 + 23 = 20$ ✓

Add 23 to make it +ve

Understand- find mod for inverse no.

* . Finding ~~Inverse~~ modulo of Inverse no. -[as per extended Euclidean algo.]

1. ~~4~~ 4^{-1} mod 23.

$4 \times \underline{?} \bmod 23 = 1$ ✓ should be satisfied.

may start from 1 upto 22 (23-1), keep on testing

$4 \times \underline{1} \bmod 23 = 1$ ✗

⋮

$4 \times 6 \bmod 23 = 1$ ✓

$\rightarrow 24 \bmod 23 = 1$

Understand- find mod for inverse no.

$3^{-1} \bmod 5$

$3 \times \_ \bmod 5 = 1$

$3 \times \underline{2} \bmod 5 = 1$ ✓.

$\therefore 3^{-1} \bmod 5 = \boxed{2}$.

above method is valid when 'n' is prime

Co-prime ⇒ gcd (5, 9) = 1.

gcd of x & n should be 1.

$5^{-1} \bmod 9$

$5 \times \_ \bmod 9 = 1$

$5 \times \underline{2} \bmod 9 = 1$.

$5^{-1} \bmod 9 = \boxed{2}$

3. $11^{-1} \bmod 26$.

$11 \times \_ \bmod 26 = 1$

$11 \times 19 \bmod 26 = 1$

$209 \bmod 26 = 1$ ✓.

$11^{-1} \bmod 26 = \boxed{19}$

Refer, Forouzan - Chapter 2. for Modular Arithmetic, Congruence and Matrices.

Group

$G = < Z_n, + >$

- A set of elements with a binary operation (.)whose result is also in the set and
- Has following properties:
  - Closure: if a and b are in set G, then c=b.a will always result in value which is in set G
  - Associative law: (a.b).c = a.(b.c) $(a+b)+c = a+(b+c)$
  - Has identity e: e.a = a.e = a $a+0=a$
  - Has inverse a': a.a' = e $a+(-a)=0$
- If commutative a.b = b.a $a+b=b+a$
  - then forms an **abelian group**

A Group - example

$in\ Z_n\ we\ can\ perform + and\ -$

$G < Z_n, + >\ is\ Abelian\ Group$

$G < Z_n, * >\ is\ not\ Abelian\ Group$

$Z_6 = \{0,1,2,3,4,5\} \quad G = < Z_n, + > \quad \boxed{G = < Z_n, * >}$

$$a = 3, b = 5, c = (a + b)\ mod\ n$$
$$c = (3 + 5) mod\ 6$$
$$c = (8) mod\ 6$$
$$c = 2$$

$$\boxed{\begin{array}{l} c = (3 * 5) mod\ 6 \\ c = (15) mod\ 6 \\ c = 3 \end{array}}$$

$$((3 + 5) + 2) mod\ 6 = (3 + (5 + 2)) mod\ 6$$
$$((8mod6) + 2) mod\ 6 = (3 + (7mod6) mod\ 6)$$
$$(2 + 2) mod\ 6 = (3 + 1) mod\ 6$$
$$(4) mod\ 6 = (4) mod\ 6$$

$$\boxed{\begin{array}{c} ((3 * 5) * 2) mod\ 6 = (3 * (5 * 2)) mod\ 6 \\ ((15mod6) * 2) mod\ 6 = (3 * (10mod6) mod\ 6) \\ (3 * 2) mod\ 6 = (3 * 4) mod\ 6 \\ (06) mod\ 6 = (12) mod\ 6 \\ 0 = 0 \end{array}}$$

$$(3 + 0) mod\ 6 = 3$$
$$\boxed{(3 * 1) mod\ 6 = 3}$$

$$(4 + (-4)) mod\ 6 = 0$$
$$(4 + (-4\ mod\ 6)) mod\ 6 = 0$$
$$(4 + (2)) mod\ 6 = 0$$
$$(6) mod\ 6 = 0$$

$$\boxed{\begin{array}{r} (4 * (4^{-1})) mod\ 6 = 1 \\ \gcd(6,4) = 2 \end{array}}\ ✗$$

$$(3 + 2) mod\ 6 = (2 + 3) mod\ 6$$
$$(5) mod\ 6 = (5) mod\ 6$$

$$\boxed{\begin{array}{c} (3 * 2) mod\ 6 = (2 * 3) mod\ 6 \\ (6) mod\ 6 = (6) mod\ 6 \end{array}}$$

Zn	+	*
Closure	✓	✓
Associative	✓	✓
Identity	✓	✓
Inverse	✓	✗
Commutative	✓	✓

A Field

$F = < Z_p, +, * >$

- A set of elements with two binary operations whose result is also in the set and
- Has following properties:
  - It's an Abelian Group for Addition Operation
  - It's an Abelian Group for Multiplication Operation
  - Identity of 1st operation has no inverse in 2nd operation.

+	*
Closure	Closure
Associative	Associative
Identity	Identity
Inverse	Inverse
Commutative	Commutative

A Field - example

$Z_7 = \{0,1,2,3,4,5,6\}$ $\boxed{F = < Z_p, +, * >}$ $Z_{7^*} = \{1,2,3,4,5,6\}$

P represents prime numbers

A Field - example

$in\ Z_p\ we\ can\ perform +, -, *\ and\ \div$

$Z_7 = \{0,1,2,3,4,5,6\}$ $\boxed{F = < Z_p, +, * >}$ $Z_{7^*} = \{1,2,3,4,5,6\}$

P represents prime numbers

$(3 + 0) mod\ 7 = 3$

$\boxed{(3 * 1) mod\ 7 = 3}$

$$(4 + (-4)) mod\ 7 = 0$$
$$(4 + (-4\ mod\ 7)) mod\ 7 = 0$$
$$(4 + (3)) mod\ 7 = 0$$
$$(7) mod\ 7 = 0$$

$$\boxed{\begin{aligned} (4 * (4^{-1})) mod\ 7 &= 1 \\ gcd(7,4) &= 1 \end{aligned}}$$ ✓

q	r_1	r_2	r	t_1	t_2	t
1	7	4	3	0	1	-1
1	4	3	1	1	-1	2
3	3	1	0	-1	2	-7
	1	0		2	-7	

Extended Euclidean to find the value of 4^{-1} in $mod\ 7$

$$\boxed{\begin{aligned} (4 * (4^{-1})) mod\ 7 &= 1 \\ gcd(7,4) &= 1 \\ (4 * (2)) mod\ 7 &= 1 \\ (8) mod\ 7 &= 1 \end{aligned}}$$

Zn	+	*
Closure	✓	✓
Associative	✓	✓
Identity	✓	✓
Inverse	✓	✓
Commutative	✓	✓

Finding Inverse Numerical 1

ex. 2. $E_{23}(1,1)$, where $\underbrace{a=1, b=1}_{\text{coefficients}}$

from equ^n: $y^2 = x^3 + x + 1 \pmod{23}$

$p = 23$ (prime no.) $(0 \ldots 22)$

i. $P = (13, 7)$ then find $-P$ → additive inverse.

$-P = (x, -y)$

$= (13, -7)$

add mod 23 to $(-7) = 16$.

$= (13, 16)$

[in modular arithmetic, we don't use -ve no.s, convert that to +ve no.

∴ $-7 \bmod 23$ i.e. $23 - 7 = 16$.]

Addition rules

Addition in elliptic curve arithmetic;

If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$

with $P \neq Q$

then, $R = P + Q = (x_R, y_R)$

where,

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

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

$\lambda =$ slope of the elliptic curve

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

Addition numerical

- $P = (3,10)$, $Q = (9,7)$, $E_{23}(1,1)$

Addition Numerical

ex.

$P = (3, 10)$, $Q = (9, 7)$ in

$x_P \quad y_P \qquad x_Q \quad y_Q$

$E_{23}(1,1)$ [of the form $E_p(a,b)$]

$p \quad a \quad b$

i] Find P+Q. Addition.

Sol: Here, $P \neq Q$.

So, $\lambda = \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \bmod p.$

$= \left(\frac{7-10}{9-3}\right) \bmod 23.$

$= \left(\frac{-3}{6}\right) \bmod 23 = \left(-\frac{1}{2}\right) \bmod 23.$

$= -2^{-1} \bmod 23. = -(12 \,\%\, 23)$

$= -(-11) \bmod 23 \qquad = 23 - 12 = 11$

$= 11 \bmod 23 = 11.$ for per.

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

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

$= (121 - 12) \bmod 23$

$= 109 \bmod 23$

$x_R = 17.$

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

$= (11(3 - 17) - 10) \bmod 23$

$= (11(-14) - 10) \bmod 23$

$= (-154 - 10) \bmod 23.$

$= -164 \bmod 23$

$= 20 \bmod 23$

$= 20.$ –ve no. is not allowed

So, find no. in multiples of 23 which is > 164 and subtract 164 from that no.

Hint

$23 \times 7 = 161$

$23 \times 8 = 184$

$184 - 164 = 20$

Multiplication Numerical

$\therefore R = P+Q = (17, 20)$

$\uparrow x_R \quad \uparrow y_R$.

ii Multiplication in Elliptic Curve arithmetic.

2P = ~~R~~ multiplication. i.e. consider repeated addition.

$2P = P + P$.

$4P = P + P + P + P$.

Now, $P = (3, 10)$, and $P = Q$.

$$\lambda = \left(\frac{3x_P^2 + a}{2y_P}\right) \bmod p.$$

$$= \left(\frac{3(3)^2+1}{2 \times 10}\right) \bmod 23.$$

$$= \frac{28}{20} \bmod 23 = \frac{28 \bmod 23}{20}$$

$$= \frac{5}{20} \bmod 23 = \frac{1}{4} \bmod 23$$

$$= 4^{-1} \bmod 23 = 6 \bmod 23.$$

$\therefore \lambda = 6$.

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

$= (6^2 - 3 - 3) \bmod 23$.

$= (36 - 6) \bmod 23$.

$= 30 \bmod 23$.

$x_R = 7$.

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

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

$= (6(-4) - 10) \bmod 23$

$= (-24 - 10) \bmod 23$

$= -34 \bmod 23$.

$y_R = 12$

$2P = (7, 12)$.

Hint

$23 \times 2 = 46$

$46 - 34 = 12$

Multiplication Numerical

$\therefore R = P+Q = (17, 20)$

$\uparrow$ x_R $\uparrow$ y_R.

ii Multiplication in Elliptic Curve arithmetic.

2P = ~~RN~~ multiplication. i.e. consider repeated addition.

$2P = P + P$.

$4P = P + P + P + P$.

Now, $P = (3, 10)$, and $P = Q$.

$$\lambda = \left(\frac{3x_p^2 + a}{2y_p} \right) \bmod p.$$

$$= \left(\frac{3(3)^2 + 1}{2 \times 10} \right) \bmod 23.$$

$$= \frac{28}{20} \bmod 23 = \frac{28 \bmod 23}{20}$$

$$= \frac{5}{20} \bmod 23 = \frac{1}{4} \bmod 23$$

$$= 4^{-1} \bmod 23 = 6 \bmod 23.$$

$\therefore \lambda = 6.$

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

$$= (6^2 - 3 - 3) \bmod 23.$$

$$= (36 - 6) \bmod 23.$$

$$= 30 \bmod 23$$

$x_R = 7.$

$$y_R = (\lambda(x_p - x_R) - y_p) \bmod p$$

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

$$= (6(-4) - 10) \bmod 23$$

$$= (-24 - 10) \bmod 23$$

$$= -34 \bmod 23.$$

$y_R = 12$

$2P = (7, 12)$.

Hint

$23 \times 2 = 46$

$46 - 34 = 12$

Numerical - 2

ex. 2. Given $y^2 = x^3 + 2x + 3 \mod 17$.

Point $P = (5, 11)$

i. Find 2P.

Slope of line λ.

$$\lambda = \frac{3 \times (5)^2 + 2}{2 \times 11} \mod 17.$$

$$= \frac{75 + 2}{22} \mod 17 = \frac{77}{22} \mod 17$$

$77 \pmod{17} = 9$

$22 \mod 17 = 5$.

$$= \frac{9}{5} \mod 17 = 9 \times 5^{-1} \mod 17.$$

Now find $5^{-1} \mod 17$

$5 \times \_ \mod 17 = 1$. $\quad 17 \times 2 = 34$

$5 \times 7 \mod 17 = 1$

so, $9 \times 7 \mod 17 = 63 \% 17$

$= \underline{12}$

Find coordinates x_3, y_3.

$x_3 = (12)^2 - 5 - 5 \mod 17$.

(x_1 & x_2 are same)

$= 144 - 10 \mod 17$.

$x_3 = 134 \mod 17 = 15$.

$y_3 = 12(5 - 15) - 11 \mod 17$.

$= 12(-10) - 11 \mod 17$

$= -120 - 11 \mod 17$.

$= -131 \mod 17$.

Find $-131 \mod 17 = -(131 \% 17)$

$= -12$.

$= -12 + 17 = 5$

$\therefore y_3 = 5$.

$2P = (15, 5)$.

Numerical – 2 (cont.)

ii. Find 3P.

$3P = P \oplus 2P$.

$= (x_1, y_1) \quad (x_2, y_2)$

$(5, 11) \quad (15, 5)$

$(x_3, y_3) =$

and find (x_3, y_3)

slope of line → when $P \neq Q$.

$\lambda = \dfrac{5-11}{15-5} \bmod 17 = \dfrac{-6}{10} \bmod 17$

$= 11 \times 10^{-1} \bmod 17 =$

$10^{-1} \% 17 = 10 \times 12 \bmod 17 = 1$

$17 \times 7 = 119$

$= 11 \times 12 \bmod 17$

$= 132 \bmod 17 = \underline{13}$

Now, $x_3 = (13)^2 - 5 - 15 \bmod 17$.

$= 169 - 20 \bmod 17$

$= 149 \bmod 17$

$x_3 = 30$.

$y_3 = 13(5 - 13) - 11 \bmod 17$.

$= 13(-8) - 11 \bmod 17$

$= -115 \bmod 17 = 4$.

$3P = (13, 4)$.

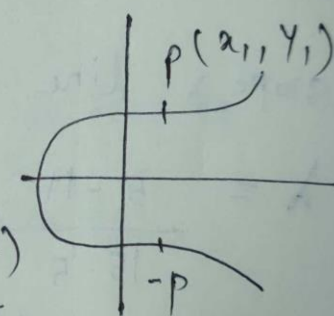
iii. Find $-P$.

$(x_1, y_1) = (5, 11)$

$(x_1, -y_1) = (5, -11+17)$

add mod 17

$-P = (5, 6)$



Elliptic Curve over $GF(2^m)$

- For elliptic curves over $GF(2^m)$, we use a cubic equation in which the variables and coefficients all take on values in $GF(2^m)$ for some number m and in which calculations are performed using the rules of arithmetic in $GF(2^m)$.
- It turns out that the form of cubic equation appropriate for cryptographic applications for elliptic curves is somewhat different for $GF(2^m)$ than for Z_p.

Elliptic Curve over GF(2^m)

- The form is
  - $y^2 + xy = x^3 + ax^2 + b$
- where it is understood that the variables x and y and the coefficients a and b are elements of GF(2^m) and that calculations are performed in GF(2^m).

Elliptic Curve over GF(2^m) – rule

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:

$$x_R = \lambda^2 + \lambda + a$$
$$y_R = x_P^2 + (\lambda + 1)x_R$$

where

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

GF(2^m)

- Computational considerations:
- A polynomial f(x) in GF(2^n) is;

  $f(X) = a_{n-1}x^{n-l} + a_{n-2}x^{n-2} + \ldots.a_1x + a_0$

- Uniquely represented by its 'n' coefficients (a_{n-1}, a_{n-2}, ………a_0). $a_i \in \{0,1\}$

❖ Thus every polynomial in GF(2^n) can be represented by an n-bit number

❖ the coefficients and variables are in finite field

GF(2^m) - basics

1 SUN

Advanced Encryption standard –
Finite Field / GF(2^n) Fields.

GF(2) = GF(2^1) = {0, 1} – power 1 for prime no. called as prime field.

GF(8) = GF(2^3) = $p^n > 1$ – $\underbrace{\text{extension}}_{\text{set of polynomials.}}$ Field.

GF(2^3) = { Contains 8 polynomial elements in this set as follows; }

8 polynomials in finite field.

000	–	$0x^2 + 0x + 0 \rightarrow 0$
001	–	$0(x^2) + 0(x) + 1 \rightarrow 1$
010	–	$0(x^2) + 1(x) + 0 \rightarrow x + 0 \rightarrow x$
011	→	$0x^2 + x + 1 \rightarrow x + 1$
100	–	$x^2 + 0 + 0 \rightarrow x^2$
101	–	$x^2 + 1$
110	→	$x^2 + x$
111	→	$x^2 + x + 1$

2 MON

$= \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$

Let, take any two elements and perform addition.

GF(2^m)

* Addition : in finite field is XOR operation.

3 TUE

1]

$$x^2 + x + 1 \qquad\qquad 1x^2 + 1x + 1$$

$$\oplus\ x^2 + x + 0 \Rightarrow \oplus\ 1x^2 + 1x + 0$$

$$\underbrace{0 + 0}_{} + 1 = 1.$$

two equal terms gets cancelled in XOR.

Addition operation result is a part of set.

2]

$$x^2 + 0 + 1$$

$$+\ x^2 + x + 0$$

$$0 + x + 1 \rightarrow x + 1 \text{ — is a part of set.}$$

4 WED

* Multiplication in GF (2^3).

$$(x^2 + x + 1)\ (x^2 + 1)$$

$$= x^4 + x^3 + x^2 + x^2 + x + 1$$

Apply addn operation with XOR

after cancellation of similar terms.

Notes

$$= x^4 + x^3 + x + 1$$

but this result doesn't appear in set

GF(2^m)

Reducing this such that will get result from existing set

Divide Result by irreducible polynomial P(x)

Divide two polynomials.

$x^4 + x^3 + x + 1$ $\downarrow$ 11011

$P(x) = x^3 + x + 1$ $\downarrow$ 1011

→ Consider mod operation.

11011 % 1011

$$
\begin{array}{r}
11 \\
1011 \overline{)\,11011} \\
\text{XOR} \rightarrow \oplus 1011 \\
\hline
01101 \\
\oplus 1011 \\
\hline
0110
\end{array}
$$

$= x^2 + x + 0 = x^2 + x$.

$x^4 + x^3 + x + 1 \% x^3 + x + 1$

$= x^2 + x$

$\downarrow$

present in set GF(2^3).

For GF(2^n) order of polynomial will never exceed $n-1$.

If case of multiplication order (power) may exceed $n-1$ then perform mod order n irreducible polynomial.

Notes

Elliptic Curve over GF(2^m)

- Find points on curve
- Reference - https://www.certicom.com/content/certicom/en/41-an-example-of-an-elliptic-curve-group-over-f2m.html

ECC Algorithm - ECDH

- ECC key exchange – similar to DH Key exchange

Global public elements

- Eq(a,b) - Elliptic curve parameters – a,b and q – prime no. or integer of the form 2^m.
- G – point on the elliptic curve

- User A key generation
  - Select private key n_A , $n_A < n$
  - Calculate public key P_A, $P_A = n_A * G$

- User B key generation
  - Select private key n_B , $n_B < n$
  - Calculate public key P_B, $P_B = n_B * G$

ECDH Algorithm

- Calculation of secret key by User A, $K = n_A * P_B$
- Calculation of secret key by User B, $K = n_B * P_A$

ECC encryption

Let the message be M

First encode this message M into a point on elliptic curve.

Let this point be P_m

- For encryption: choose a random positive integer K.
- The cipher point will be,
  - $Cm = \{KG, P_m + KP_B\}$
  - This point will be sent to receiver.

ECDH Algorithm

- For Decryption: multiply x-coordinate with receiver's secret key - $KG * n_B$
- Then subtract from coordinate of cipher point;
- $Pm + KP_B – (KG * n_B)$

- We know that, $P_B = n_B * G$

So substitute in above equation and we get,

- $Pm + KP_B – KP_B$

$_=$ Pm

So, receiver gets the same point.

ECDH - numerical

Elliptic Curve Diffie Hellman Exchange
ECDHE.

Encryption and Decryption.

Step 1: Encode a plain text msg as a point on the curve.

$M \in E_{11}(1,1)$

$(4,6) \rightarrow$ plain text msg.

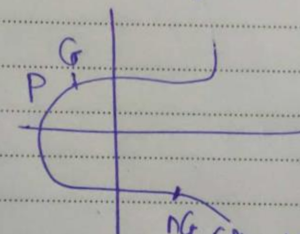
Step 2: Establish public key and private key.

Choose generator point $G \in E_p(a,b)$.

$(1,5) \in E_{11}(1,1)$

Select private key n.

value of n should be between 1 to 10.



$nG\ (x_3, y_3)$ = Public key.

Compute the public key $P_U = nG$.

Let $n = 2$ = private key.

$P_u = 2G = \cancel{G} + G.$

$= (1,5) + (1,5).$

Use case 2.

algebraic eqn:

ECDH – numerical (cont.)

2012 January

13 FRI

$$\lambda = \frac{3(1)^2+1}{2\times 5} \bmod 11 = \frac{4}{10} \bmod 11$$

$$= 4.(10^{-1}) \bmod 11 = 4\,(10^{-1} \bmod 11)$$

$$\lambda = 4 \times 10 \bmod 11 = 40 \bmod 11 = 7.$$

$$x_3 = (7)^2 - 1 - 1 \bmod 11$$

$$= 49 - 2 \bmod 11 = 47 \bmod 11 = 3.$$

$$y_3 = 7(1-3) - 5 \bmod 11$$

$$= 7(-2) - 5 \bmod 11 = -19 \bmod 11 = 3.$$

$(x_3, y_3) = 2G = (3,3) =$ Public key.

14 SAT

Step 3: Encrypt the msg using the public key.

$C = [\,(kG),\ (M + kP_U)\,]$ k is random no. between 1 to p-1 = 1 to 10.

Let $k = 2$.

$$\therefore C = [\,\underbrace{(2\,(1,5))}_{C_1},\ \underbrace{[(4,6) + 2(3,3)]}_{C_2}\,]$$

Notes

ECDH – numerical (cont.)

$C_1 = 2(1,5) = (1,5) + (1,5) = (3,3)$ 15 SUN

$C_2 = (4,6) + 2(3,3) = (4,6) + (3,3) + (3,3)$

Compute $(3,3) + (3,3)$

$\lambda = \frac{3 \times 3^2 + 1}{2 \times 3} \bmod 11 = \frac{23}{6} \bmod 11$

$= 23 \cdot (6)^{-1} \bmod 11 = 1.$

$x_3 = 1 - 3 - 3 \bmod 11 = 1 - 6 \bmod 11$

$= -5 \bmod 11 = (11 - 5) = 6$ 16 MON

$y_3 = 1(3 - 6) - 3 \bmod 11$

$= -3 - 3 \bmod 11 = -6 \bmod 11 = 5.$

$(x_3, y_3) = (6, 5).$

$\therefore C_2 = (4,6) + (6,5)$

Compute $(4,6) + (6,5)$

$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{5 - 6}{6 - 4} = \frac{-1}{2} \bmod 11$

Notes

$= -1 (2)^{-1} \bmod 11 = 5.$

ECDH – numerical (cont.)

17 TUE

$x_3 = 5^2 - 4 - 6 \mod 11$

$= 25 - 10 \mod 11 = 15 \mod 11 = 4.$

$y_3 = \lambda (x_1 - x_3) - y_1 \mod 11$

$= 5(4 - 4) - 6 \mod 11$

$= 0 - 6 \mod 11 = 5.$

$(x_3, y_3) = (4, 5).$

$\therefore C_2 = (4, 5).$

$\therefore C = [(3,3), (4,5)].$

18 WED

this is encryption in ECC.

Step 4: Decrypt using private key.

$M = C_2 - [nC_1]$

$= (4,5) - [2 \times (3,3)].$

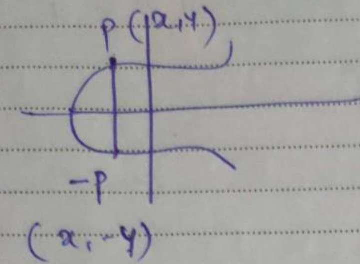
$= (4,5) - [(3,3) + (3,3)]$

$= (4,5) - (6,5).$

Notes

ECDH – numerical (cont.)

Recall, Additive inverse of P is −P.



So, $M = (4,5) - (6,5)$

$= (4,5) + [-(6,5)]$

$= (4,5) + [(6,-5)]$

$(6,-5) \bmod 11$

Solve, $-5 \bmod 11 = 6$.

∴ it is $(6,6)$

$= (4,5) + (6,6)$.

$\lambda = \frac{6-5}{6-4} \bmod 11 = \frac{1}{2} \bmod 11 = 2^{-1} \bmod 11$

$= 6$.

$x_3 = 6^2 - 4 - 6 \bmod 11 = 26 \bmod 11 = 4$.

$y_3 = 6(4-4) - 5 \bmod 11 = -5 \bmod 11$

$= 6$.

ECDH – numerical (cont.)

21 SAT

$\therefore (x_3, y_3) = (4, 6) =$ plaintext msg M.

Factoring with Elliptic Curves

Basis idea: To factorize an integer n choose an elliptic curve E, a point P on E and compute (modulo n) either iP for $i = 2, 3, 4, \dots$ or $2^j P$ for $j = 1, 2, \dots$. The point is that in doing that one needs to compute gcd(k,n) for various k. If one of these values is between 1 and n we have a factor of n.

Factoring of large integers: The above idea can be easily parallelised and converted to using an enormous number of computers to factor a single very large n. Each computer gets some number of elliptic curves and some points on them and multiplies these points by some integers according to the rule for addition of points. If one of computers encounters, during such a computation, a need to compute $1 < gcd(k, n) < n$, factorization is finished.

Example: If curve $E : y^2 = x^3 + 4x + 4 \pmod{2773}$ and its point $P = (1, 3)$ are used, then $2P = (1771, 705)$ and in order to compute 3P one has to compute $gcd(1770, 2773) = 59$ – factorization is done.

Example: For elliptic curve $E : y^2 = x^3 + x - 1 \pmod{35}$ and its point $P = (1, 1)$ we have $2P = (2, 2); 4P = (0, 22); 8P = (16, 19)$ and at the attempt to compute 9P one needs to compute $gcd(15, 35) = 5$ and factorization is done.

Factoring with Elliptic Curves - example

Step 1. Generate an elliptic curve with point P mod n

$$y^2 = x^3 + 10x - 2 \pmod{4453} \; let \; P = (1,3)$$

Step 2. Compute BP for some integer B.

$$Lets \;\; compute \;\; 2P \;\; first \;\; \frac{3x^2+10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}$$

$$We \; used \; the \; fact \; that \;\; \gcd(6,4453) = 1 \; to \; find \; 6^{-1} \equiv 3711 \pmod{4453}$$

$$we \; find \; that \; 2P = (x,y) \; with \; x \equiv 3713^2 - 2 \;\; y \equiv -3713(x-1) - 3 \equiv 3230$$

$2P \; is \; (4332, 3230)$

Ex: We want to factor 4453

Factoring with Elliptic Curves – example (cont.)

Step 3. If step 2 fails because some slope does not exist mod n, the we have found a factor of n.

$$\textit{To compute } 3P \textit{ we add } P \textit{ and } 2P$$

$$\textit{The slope is } \frac{3230-3}{4332-1} = \frac{3227}{4331}$$

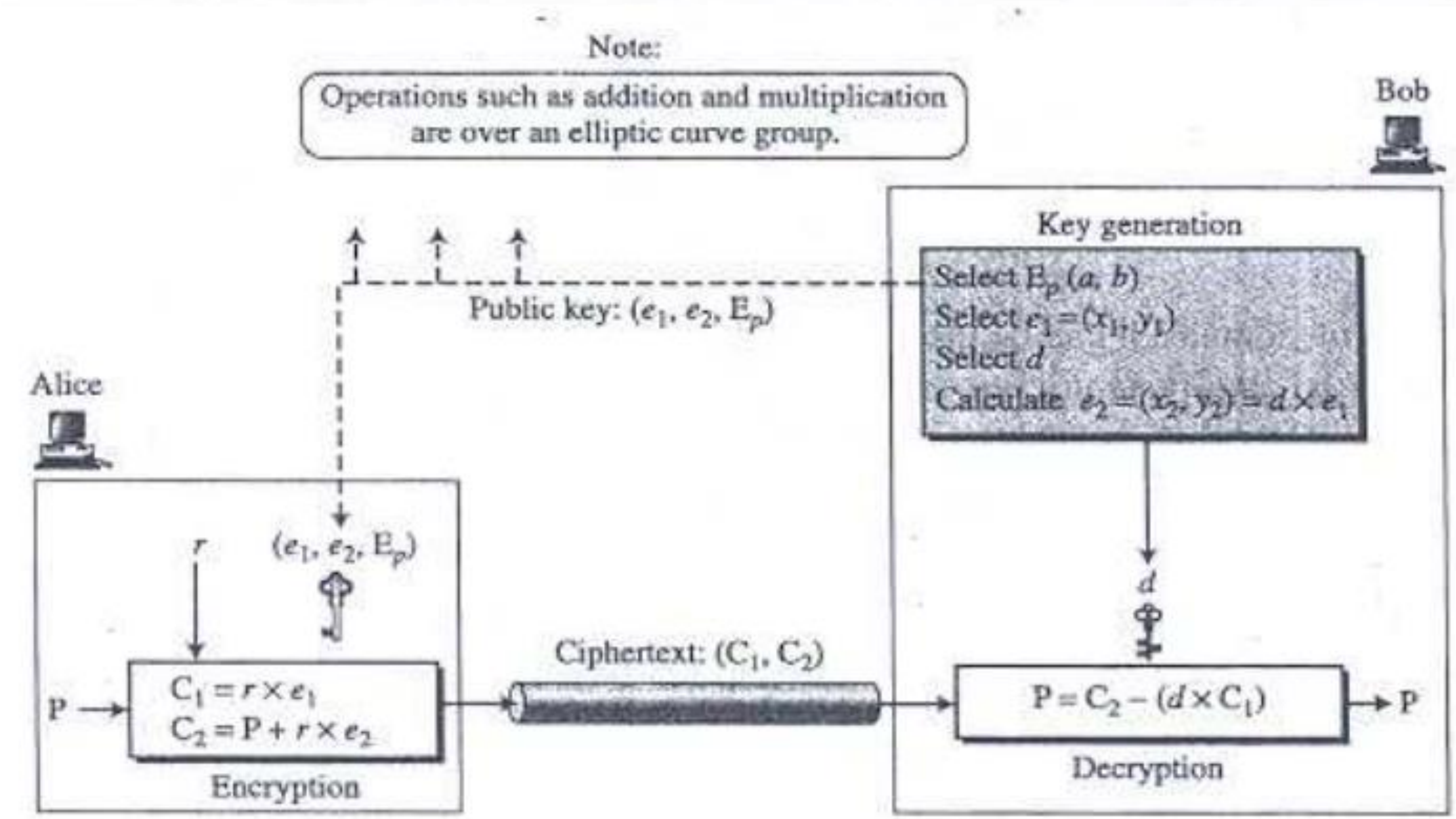
$$\textit{But} \quad \gcd(4331, 4453) = 61 \neq 1 \ \ \textit{we can not find } 4331^{-1} (\bmod 4453)$$

$$\textit{However, we have found the factor } 61 \textit{ of } 4453$$

Elliptic Curve Cryptography Simulating ElGamal

ElGamal with Elliptic Curve

Figure 10.16 *ElGamal cryptosystem using the elliptic curve*



ElGamal with Elliptic Curve (cont.)

Generating Public and Private Keys

1. Bob chooses E(a, b) with an elliptic curve over **GF**(p) or **GF**(2^n).
2. Bob chooses a point on the curve, $e_1(x_1, y_1)$.
3. Bob chooses an integer d.
4. Bob calculates $e_2(x_2, y_2) = d \times e_1(x_1, y_1)$. Note that multiplication here means multiple addition of points as defined before.
5. Bob announces E(a, b), $e_1(x_1, y_1)$, and $e_2(x_2, y_2)$ as his public key; he keeps d as his private key.

Encryption

Alice selects P, a point on the curve, as her plaintext, P. She then calculates a pair of points on the text as ciphertexts:

$$C_1 = r \times e_1 \qquad C_2 = P + r \times e_2$$

ElGamal with Elliptic Curve (cont.)

Decryption

Bob, after receiving C_1 and C_2, calculates P, the plaintext using the following formula.

$$P = C_2 - (d \times C_1) \quad \text{The minus sign here means adding with the inverse.}$$

We can prove that the P calculated by Bob is the same as that intended by Alice, as shown below:

$$P + r \times e_2 - (d \times r \times e_1) = P + (r \times d \times e_1) - (r \times d \times e_1) = P + O = P$$

P, C_1, C_2, e_1, and e_2 are all points on the curve. Note that the result of adding two inverse points on the curve is the *zero point*.

ElGamal with Elliptic Curve - Numerical

Example 10.19

Here is a very trivial example of encipherment using an elliptic curve over **GF**(p).

1. Bob selects $E_{67}(2, 3)$ as the elliptic curve over **GF**(p).
2. Bob selects $e_1 = (2, 22)$ and $d = 4$.
3. Bob calculates $e_2 = (13, 45)$, where $e_2 = d \times e_1$.
4. Bob publicly announces the tuple (E, e_1, e_2).
5. Alice wants to send the plaintext $P = (24, 26)$ to Bob. She selects $r = 2$.
6. Alice finds the point $C_1 = (35, 1)$, where $C_1 = r \times e_1$.
7. Alice finds the point $C_2 = (21, 44)$, where $C_2 = P + r \times e_2$.
8. Bob receives C_1 and C_2. He uses $2 \times C_1$ $(35, 1)$ to get $(23, 25)$.
9. Bob inverts the point $(23, 25)$ to get the point $(23, 42)$.
10. Bob adds $(23, 42)$ with $C_2 = (21, 44)$ to get the original plaintext $P = (24, 26)$.

References

- William Stalling
- Forouzan