Network Security

Network security is protection of the access to files and directories in a computer **network** against hacking, misuse and unauthorized changes to the system.

Definition I

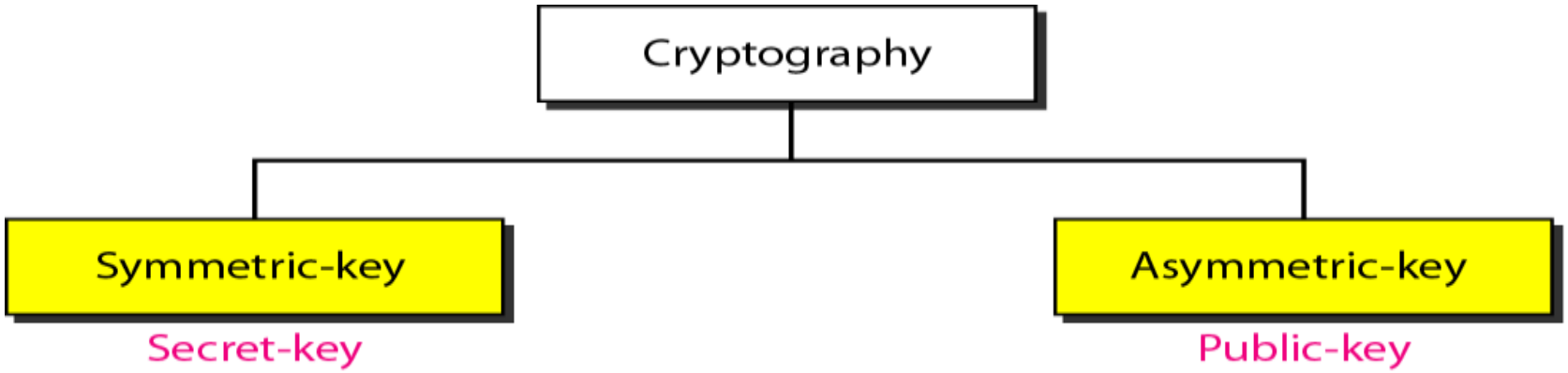
Definition II

Network security is a set of rules and configurations designed to protect the integrity, confidentiality and accessibility of computer networks

Four Factor

1. **Privacy:**The sender and the receiver expect confidentiality.
2. **Authentication:** The receiver is sure of the sender's identity and that an imposter has not sent the message.
3. **Integrity:** The data must arrive at the receiver exactly as it was sent. Non-
4. **Reputation:** The receiver must able to prove that a received message came from a specific sender.

Types



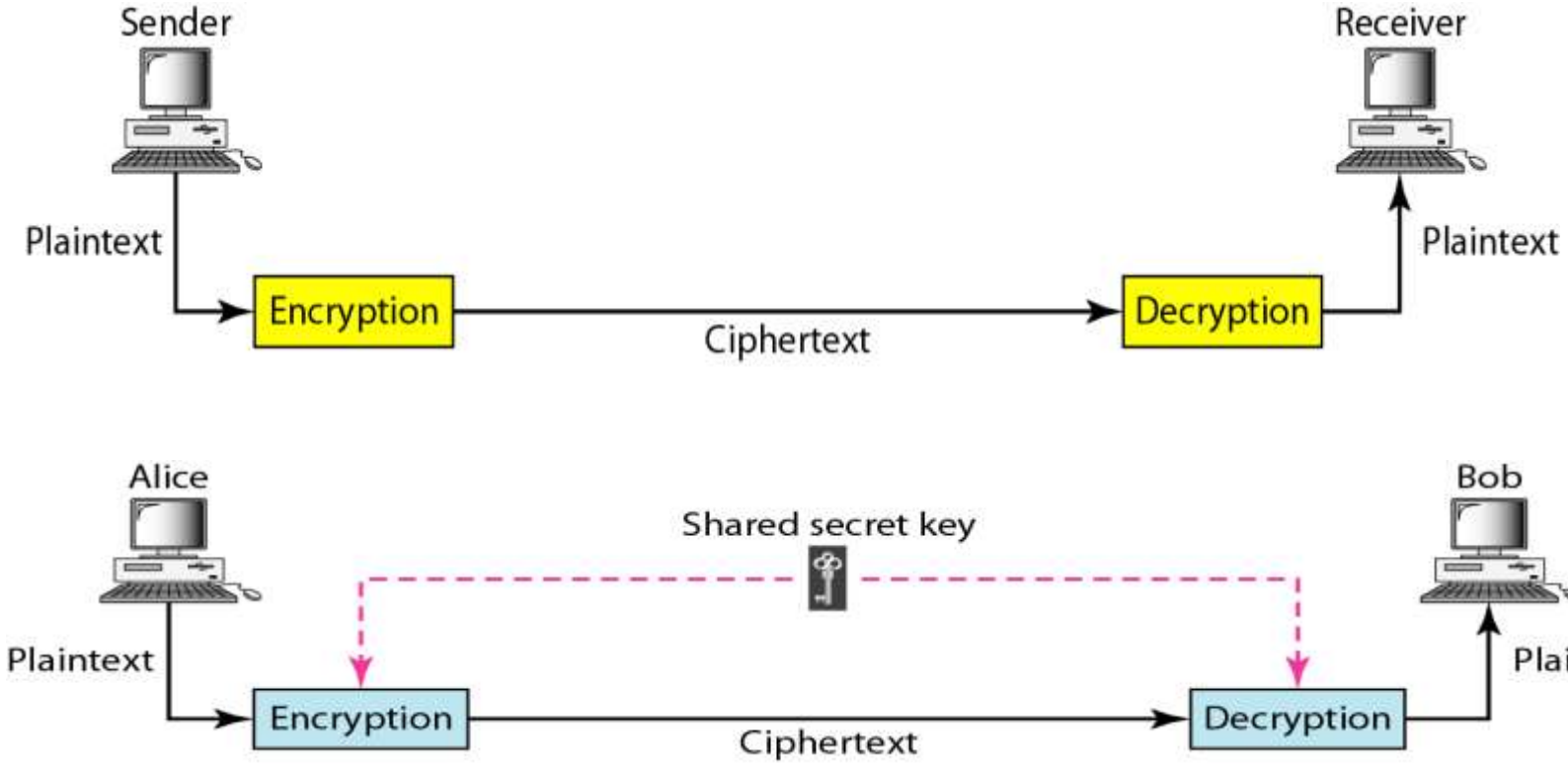
Symmetric-key cryptography

Asymmetric-key cryptography

Symmetric-key cryptography

In symmetric-key cryptography, the same key is used by the sender(for encryption) and the receiver (for decryption).

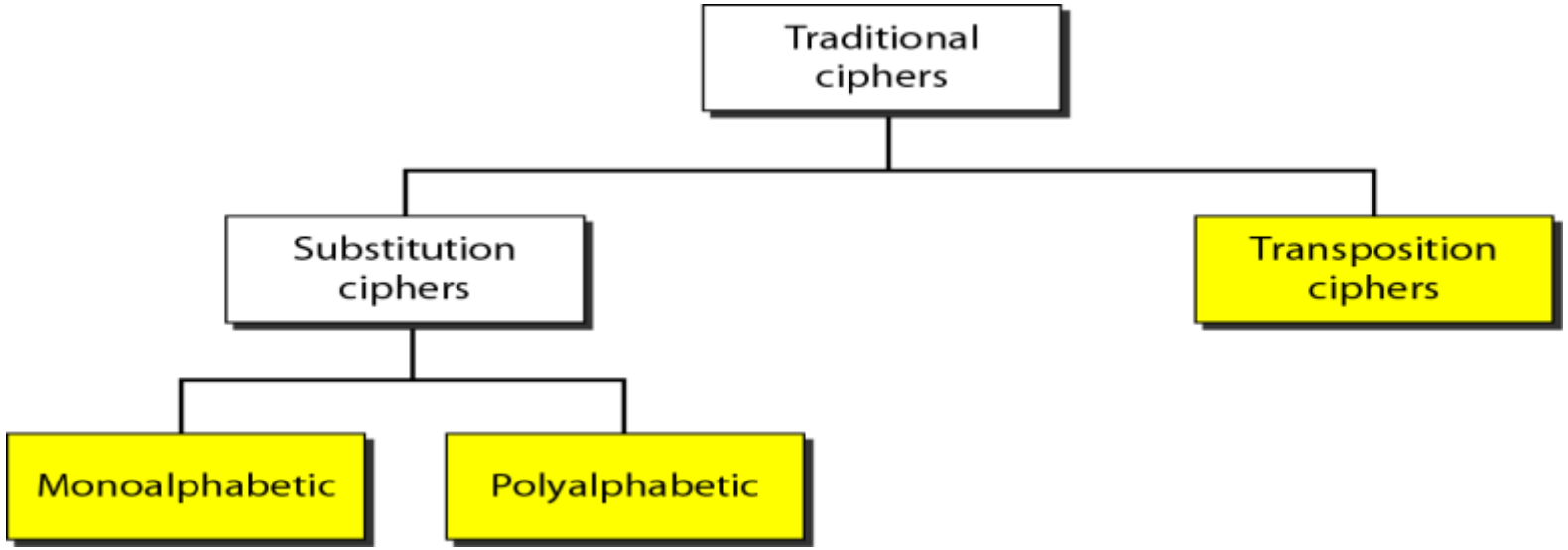
The key is shared.
Algorithm: DES,3DES



Symmetric-key cryptography

General idea of traditional cipher

Symmetric-key cryptography



A substitution cipher replaces one symbol with another.

An example key for mono-alphabetic substitution cipher

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	N	O	A	T	R	B	E	C	F	U	X	D	Q	G	Y	L	K	H	V	I	J	M	P	Z	S	W

We can use the key to encrypt the message

this message is easy to encrypt but hard to find the key

The ciphertext is

ICFVQRVVNEFVRNVSIYRGAHSLIOJICNHTIYBFGTICRXRS

Substitution Cipher

Plaintext →	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext →	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Value →	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Example

Use the additive cipher with key = 15 to encrypt the message “hello”.

Solution

We apply the encryption algorithm to the plaintext, character by character. The result is “WTAAD”. Note that the cipher is mono alphabetic because two instances of the same plaintext character (ls) are encrypted as the same character (A).

Plaintext: h → 07	Encryption: (07 + 15) mod 26	Ciphertext: 22 → W
Plaintext: e → 04	Encryption: (04 + 15) mod 26	Ciphertext: 19 → T
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: l → 11	Encryption: (11 + 15) mod 26	Ciphertext: 00 → A
Plaintext: o → 14	Encryption: (14 + 15) mod 26	Ciphertext: 03 → D

Example

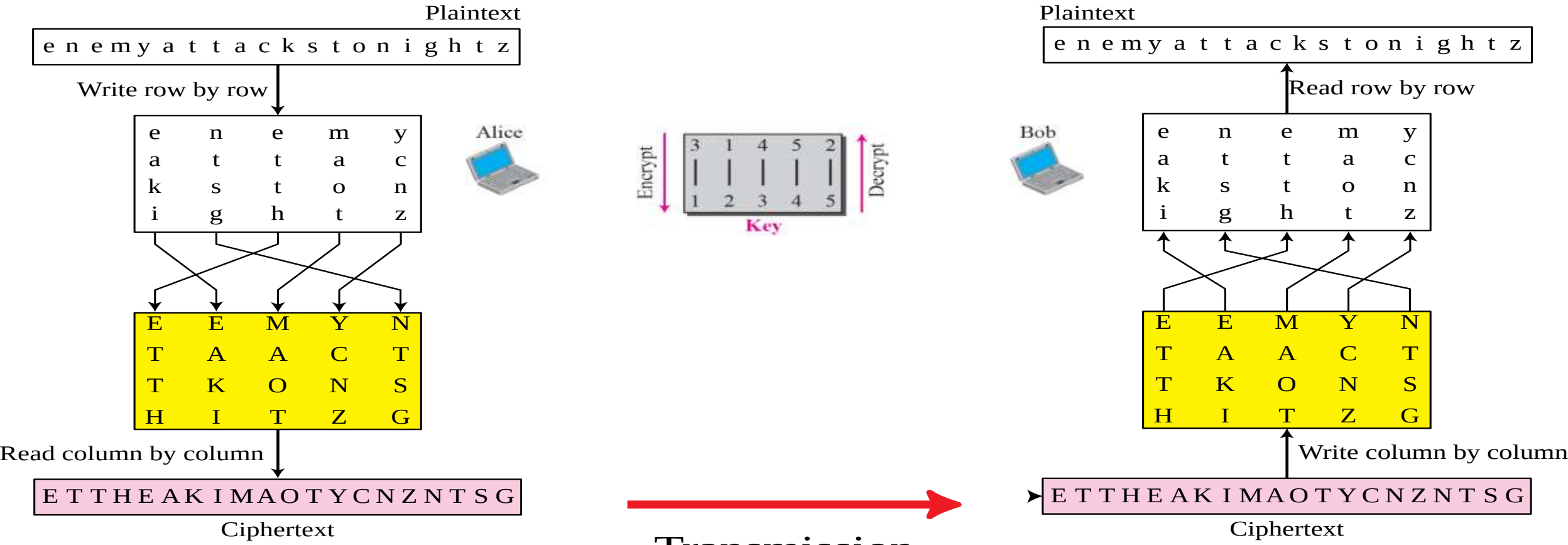
Use the additive cipher with key = 15 to decrypt the message “WTAAD”.

Solution

We apply the decryption algorithm to the plaintext character by character. The result is “hello”. Note that the operation is in modulo 26, which means that we need to add 26 to a negative result (for example -15 becomes 11).

Ciphertext: W → 22	Decryption: (22 – 15) mod 26	Plaintext: 07 → h
Ciphertext: T → 19	Decryption: (19 – 15) mod 26	Plaintext: 04 → e
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: A → 00	Decryption: (00 – 15) mod 26	Plaintext: 11 → l
Ciphertext: D → 03	Decryption: (03 – 15) mod 26	Plaintext: 14 → o

A transposition cipher reorders symbols.



Symmetric-key cryptography

- Advantages:
  - Simple
  - Faster
- Disadvantages:
  - Key must exchanges in secure way
  - Easy for hacker to get a key as it is passed in unsecure way.

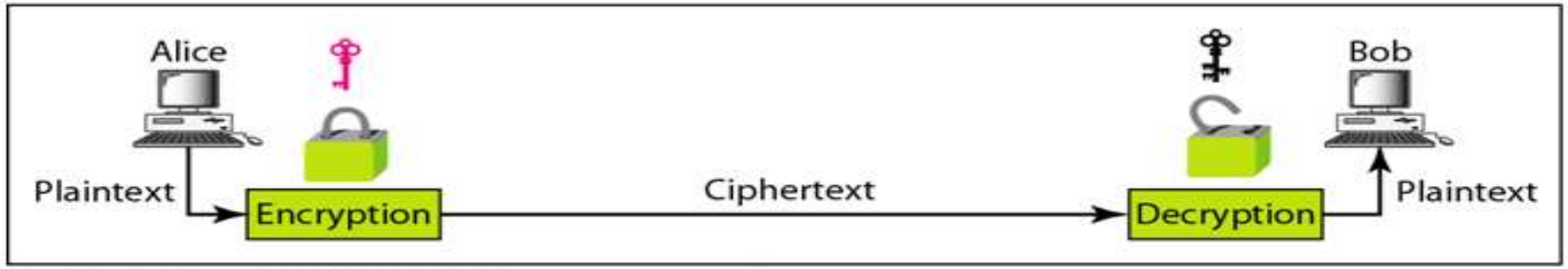
ASYMMETRIC ENCRYPTION

Asymmetric encryption use two keys, one to encrypt the data, and another key to decrypt the data.

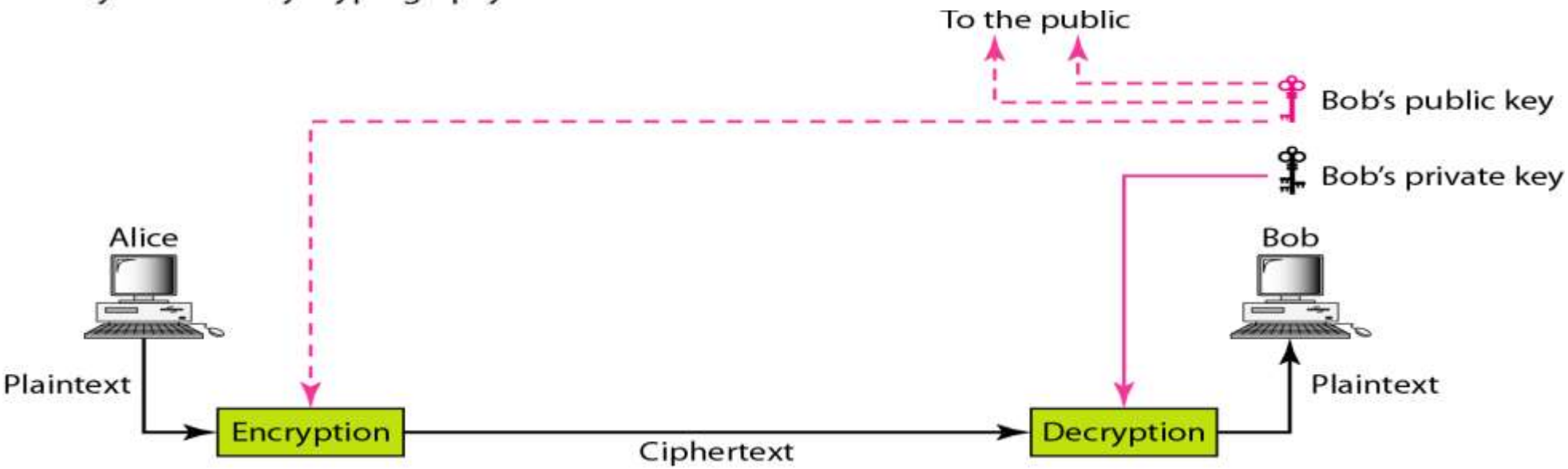
These keys are generated together.

1. One is named as Public key and is distributed freely. The other is named as Private Key and it is kept hidden.
2. Both Sender & Recipient has to share their Public Keys for Encryption and has to use their Private Keys for Decryption.

Asymmetric-key cryptography



b. Asymmetric-key cryptography



Asymmetric-key cryptography

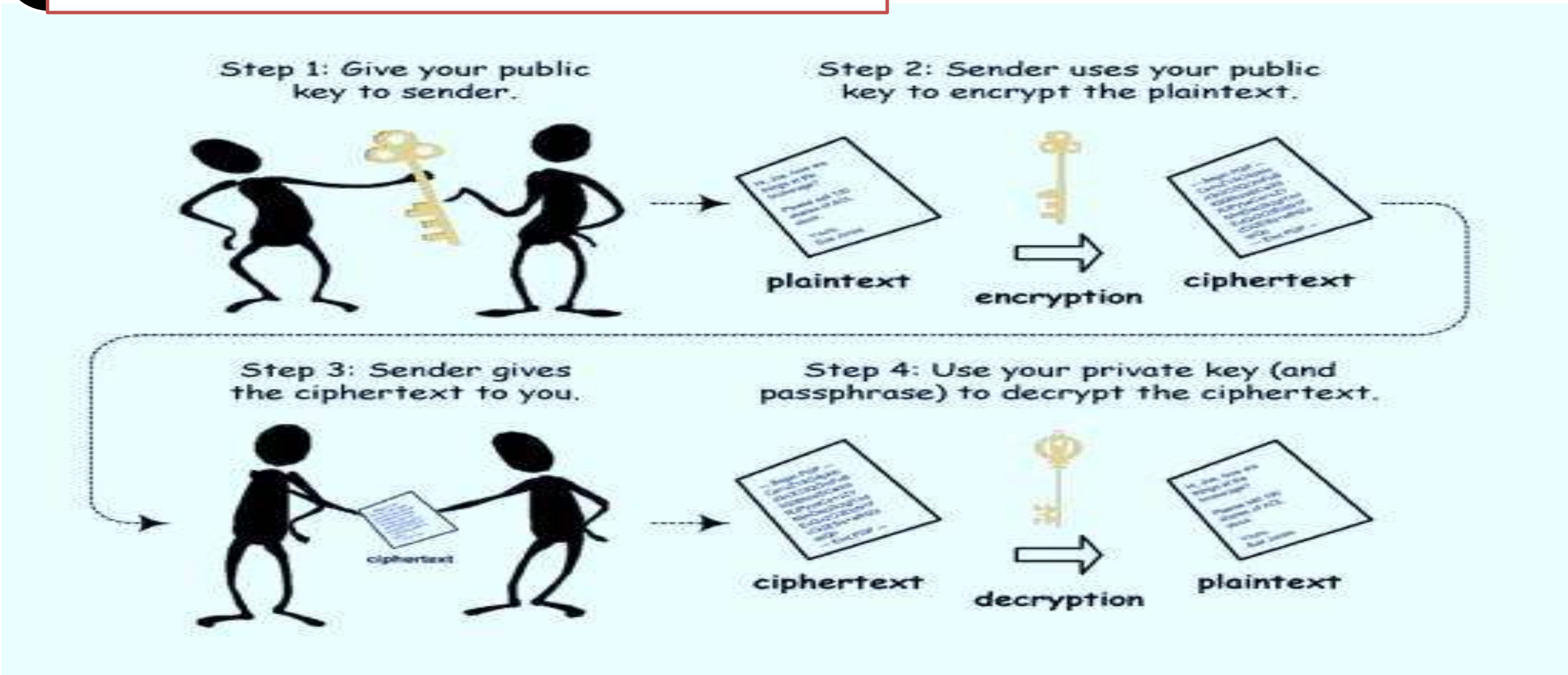
Advantages

1. More Secured
2. Authentication

Disadvantages

1. Relatively Complex

How it WORKS…….?


Step 1: Give your public key to sender.
Step 2: Sender uses your public key to encrypt the plaintext.
plaintext
encryption
ciphertext
Step 3: Sender gives the ciphertext to you.
Step 4: Use your private key (and passphrase) to decrypt the ciphertext.
ciphertext
ciphertext
decryption
plaintext

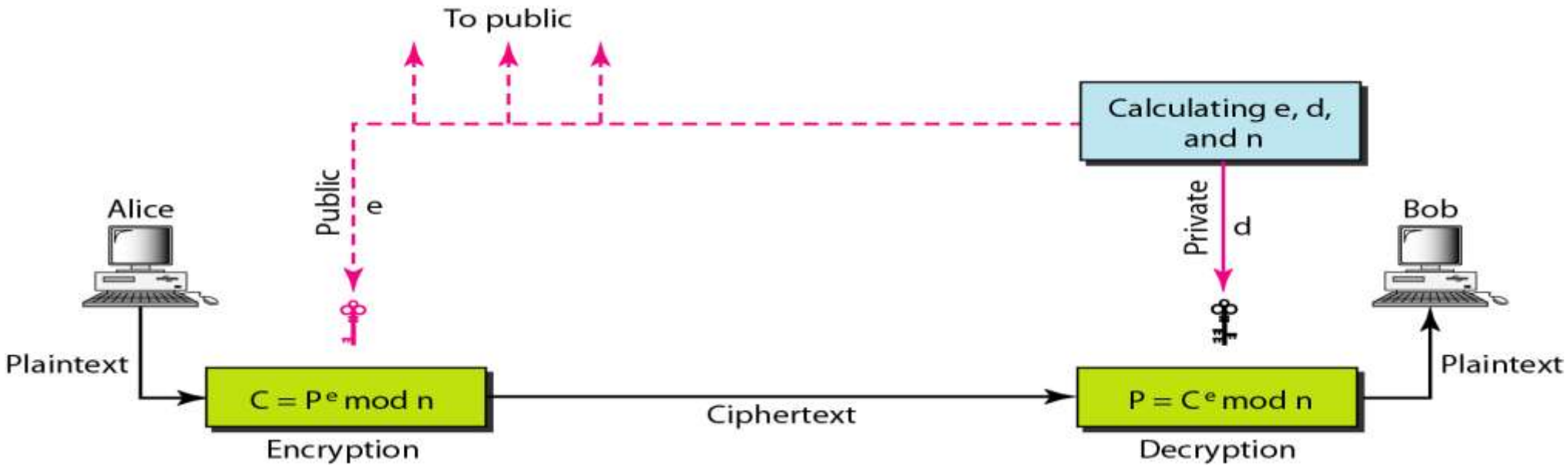
Asymmetric Encryption Algorithms

- RSA:
- Digital Signature Algorithm:
- Diffie-Helman:.

RSA

1. Most widely accepted and implemented general purpose approach to public key encryption developed by Rivest-Shamir and Adleman (RSA) at MIT university.
2. RSA scheme is block cipher in which the plaintext and ciphertext are integers between 0 and n-1 for same n.
3. Typical size of n is 1024 bits. i.e n<2.

In RSA, e and n are announced to the public; d and Φ are kept secret.



a) Key Genration :

- Select p,q…….. p and q both are the prime numbers, p≠q.
- Calculate n=p×q
- Calculate q(n) = (p-1) (q-1)
- Select integer….g(d ((n), e)) =1 & 1< e < (n)
- Calculate d; d= e-1 mod (n)
- Public Key, PU= {e, n}
- Private Key, PR ={d,n}

b) Encryption :

- Plaintext : m<n< p="">
- Ciphertext: C

c) Decryption:

- Ciphertext: C
- Plaintext : M= Cd mod n
- Note 1 : (n) -> Euler's totient function
- Note 2: Relationship between C and d is expressed as:

ed (mod (n))=1

ed = 1 mod (n)

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

- **Key Generation :**

1. Select 2 prime numbers -> p=17 and q=11
2. Calculate n = p×q =17 ×11=187
3. Calculate = 16 × 10= 160 Select 'e' such that e is relatively prime to (n)=160 and e <
4. Determine d such that :

de =1 mod (n)

d × 7 = 1 mod 160

↓

161

$d = e^{-1} \ mod \ (n)[161/7 =$

$div.\ (d)23$ and remainder (mod) =1

$d = 23$

1. Then the resulting keys are public key :

PU = {7, 187 }

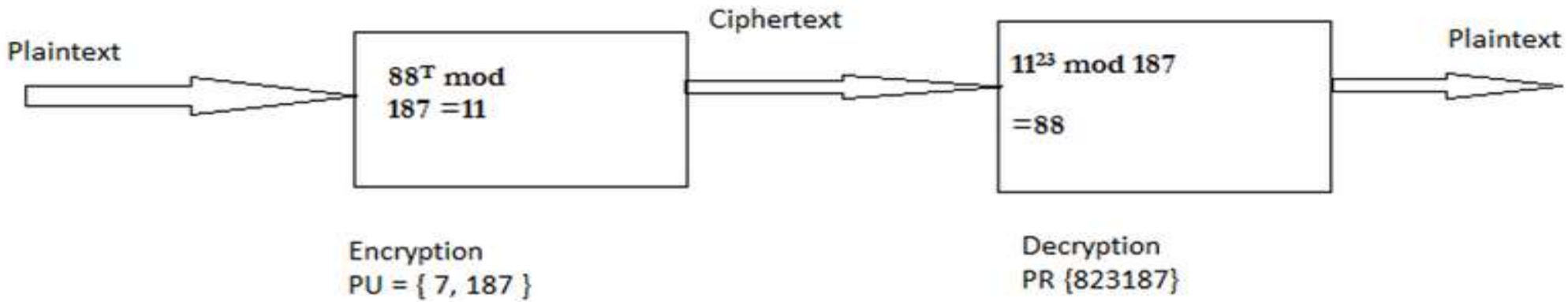
PR = {23, 187 }

Let M=88 for encryption

$$C = 88^7 mod(187)$$
$$88 mod 187 = 88$$
$$88^2 mod 187 = 7744 mod 187 = 77$$
$$88^4 mod 187 = 59969536 mod 187 = 132$$
$$88^7 mod 187 = (88^4 mod 187) \times (88^2 mod 187) \times (88 mod 187) mod 187$$
$$= (132 \times 77 \times 88) mod 187$$
$$= 894432 mod 187$$
$$= 11$$

- **For Decryption :**

$$M = C^d mod 187$$
$$= 11^{23} mod 187$$
$$11^1 mod 187 = 11$$
$$11^2 mod 187 = 121$$
$$11^4 mod 187 = 14641/187 = 55$$
$$11^8 mod 187 = 214358881 mod 187 = 33$$
$$11^{23} mod 187$$
$$= (11^8 mod 187 \times 11^8 mod 187 \times 11^4 mod 187 \times 11^2 mod 187 \times 11^1 mod 187) mod 187$$
$$= (33 \times 33 \times 55 \times 81 \times 11) mod 187$$
$$= 79720245 mod 187$$
$$= 88$$



Diffie-Hellman

The symmetric (shared) key in the Diffie-Hellman protocol is

$$K = g^{xy} \bmod p.$$

Let us give a trivial example to make the procedure clear. Our example uses small numbers, but note that in a real situation, the numbers are very large. Assume g = 7

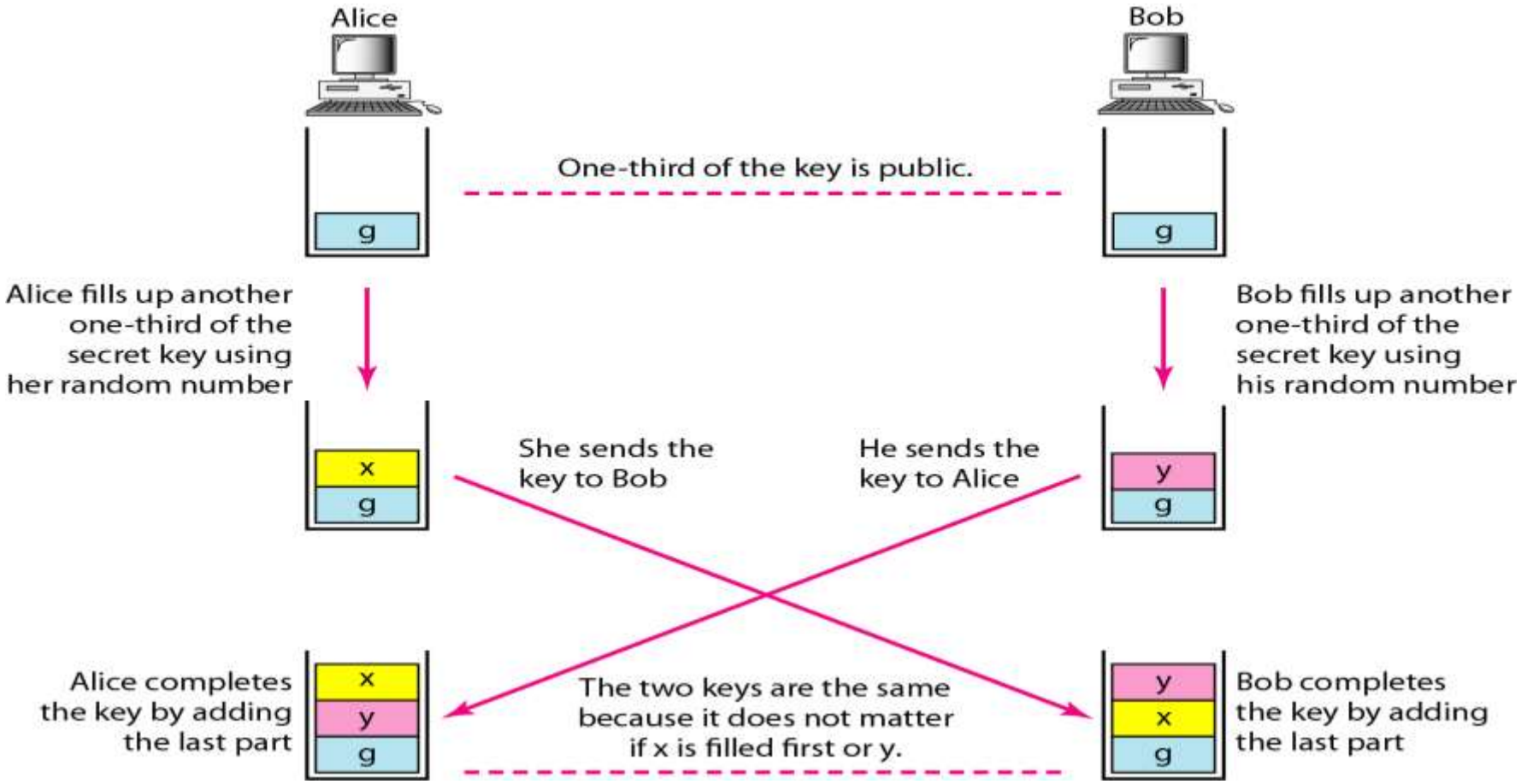
and p = 23.

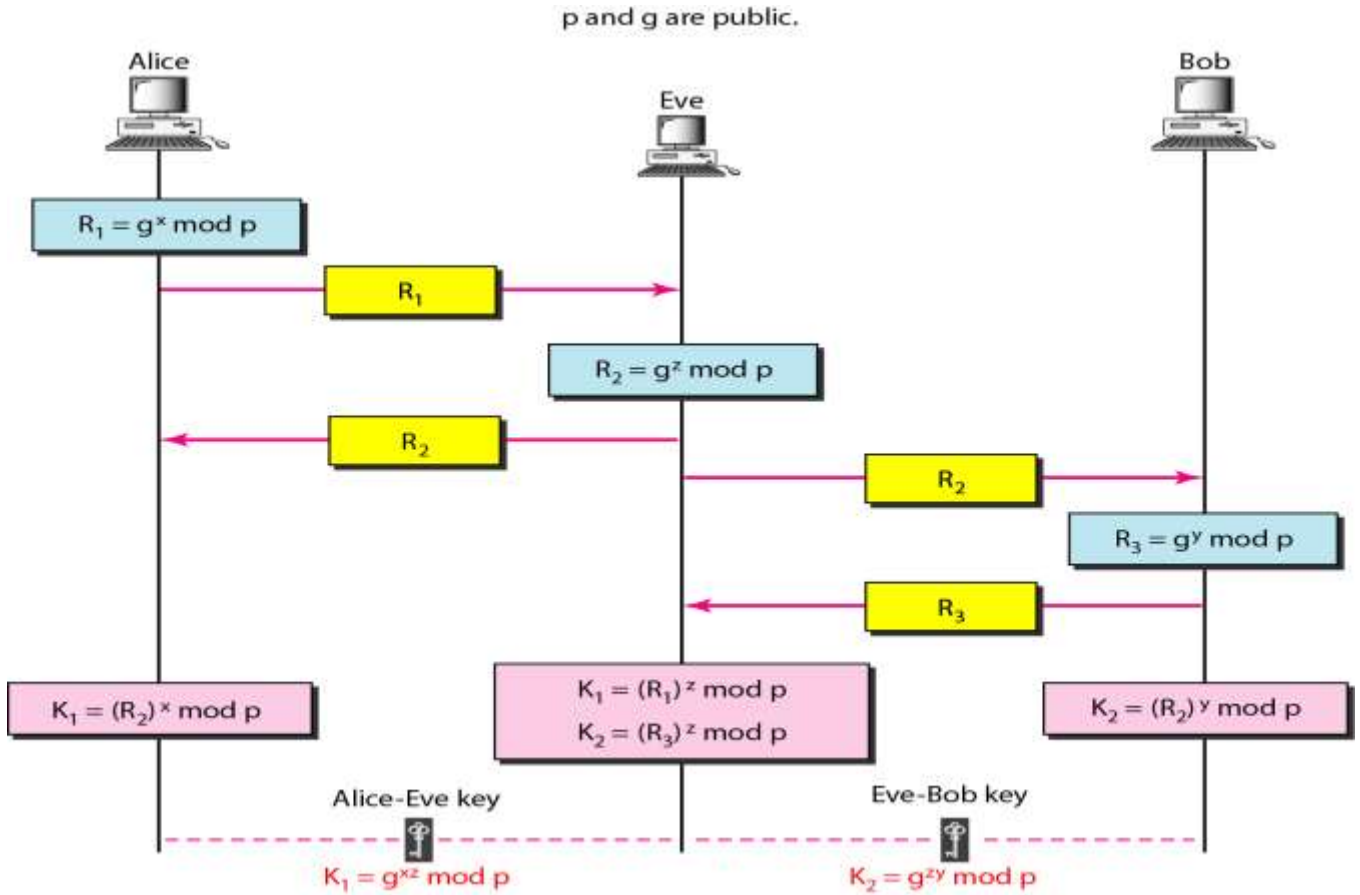
The steps are as follows:

1. Alice chooses x = 3 and calculates $R_1 = 7^3 \bmod 23 = 21$.
2. Bob chooses y = 6 and calculates $R_2 = 7^6 \bmod 23 = 4$.
3. Alice sends the number 21 to Bob.
4. Bob sends the number 4 to Alice.
5. Alice calculates the symmetric key $K = 4^3 \bmod 23 = 18$.
6. Bob calculates the symmetric key $K = 21^6 \bmod 23 = 18$.

The value of K is the same for both Alice and Bob;

$g^{xy} \bmod p = 7^{18} \bmod 23 = 18$.


Alice
Bob
One-third of the key is public.
g
g
Alice fills up another one-third of the secret key using her random number
Bob fills up another one-third of the secret key using his random number
x
g
y
g
She sends the key to Bob
He sends the key to Alice
Alice completes the key by adding the last part
x
y
g
The two keys are the same because it does not matter if x is filled first or y.
y
x
g
Bob completes the key by adding the last part


p and g are public.
Alice
Eve
Bob
$R_1 = g^x \bmod p$
R_1
$R_2 = g^z \bmod p$
R_2
R_2
$R_3 = g^y \bmod p$
R_3
$K_1 = (R_2)^x \bmod p$
$K_1 = (R_1)^z \bmod p$
$K_2 = (R_3)^z \bmod p$
$K_2 = (R_2)^y \bmod p$
Alice-Eve key
Eve-Bob key
$K_1 = g^{xz} \bmod p$
$K_2 = g^{zy} \bmod p$

Difference between Symmetric key and Asymmetric key Cryptography

Categories	Symmetric key Cryptography	Asymmetric key Cryptography
Key used for encryption /decryption	Same key is used for encryption & decryption.	One key is used for encryption & another different key is used for decryption.
Key process	Ke=Kd	Ke# Kd
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size.	More than the original clear text size.
Key agreement/exchange	A big problem	No problem at all.
Usage	Mainly used for encryption and decryption, cannot be used for digital signatures.	Can be used for encryption and decryption as well as for digital signatures.
Efficiency in usage	Symmetric key cryptography is often used for long messages.	Asymmetric key cryptography are more efficient for short messages.

Thank you