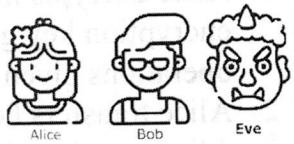
EXERCISE 1 (converting text into binary code)

1. Choose a secret four-letter word
2. Convert the chosen word into a digital (binary) code (use the **BINARY REPRESENTATION OF THE ALPHABET** table given below)



FOUR-LETTER WORD																				
BINARY CODE																				

Cryptography – field of communication that deals with the encryption of data sent over communication channels

Data Encryption – rendering a message unrecognizable, ideally making it readable only for the sender and the recipient

Random Encryption Key – a key used to encrypt the data, accessible only to legitimate end users

Key Generation: based on complex computational algorithms supposed to be "uncrackable"

Key Distribution – transferring the random encryption key to the legitimate end users

BINARY REPRESENTATION OF THE ALPHABET

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

EXERCISE 2 (encrypting binary code)

1. Alice encrypts the binary code from Exercise 1 using the secure encryption key given above. She uses the binary addition operations given in the **BINARY ADDITION TABLE.**
2. Alice transfers her encrypted message publicly to Bob and Eve.
3. Alice transfers the encryption key secretly to Bob **only**.

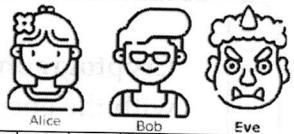
BINARY CODE																			
ENCRYPTION KEY ⊕																			
ENCRYPTED MESSAGE																			

SECURE ENCRYPTION KEY
01000 11010 11011 00101

BINARY ADDITION TABLE

0	1	0	1
+ 0	+ 0	+ 1	+ 1
= 0	= 1	= 1	= 0

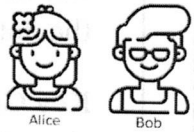
ENCRYPTED MESSAGE FROM EVE SENT TO BOB AND EVE PUBLICLY



ENCRYPTED MESSAGE																			

Can Eve figure out what Alice's word is encrypted in her message?

ENCRYPTION KEY FOR BOB ONLY



SECURE ENCRYPTION KEY
01000 11010 11011 00101

How can Alice send the encryption key to Bob secretly through public network without Eve capturing it?

EXERCISE 3 (receiving encrypted message)

1. Bob receives the encrypted message from Alice through the public channel.
2. Bob receives the encryption key from Alice secretly.
3. Bob decrypts Alice's message using the secure encryption key. He uses the binary addition operations given in the **BINARY ADDITION TABLE.**

ENCRYPTED MESSAGE ⊕																			
ENCRYPTION KEY																			
BINARY CODE																			
FOUR-LETTER WORD																			

BINARY REPRESENTATION OF THE ALPHABET

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

BINARY ADDITION TABLE

0	1	0	1
+ 0	+ 0	+ 1	+ 1
= 0	= 1	= 1	= 0

As long as Alice and Bob keep their shared key perfectly secret, there is no way for an eavesdropper to learn the message.

Note that sharing the key is different than sharing a message.

The key is a completely random binary sequence, and contains no useful information itself.

There is a risk of eavesdropper capturing the encryption key during the key distribution.

EXERCISE 3 (receiving encrypted message)

1. Eve receives the encrypted message from Alice through the public channel.
2. Can Eve decrypt the message received from Alice?

ENCRYPTED MESSAGE																				
FOUR-LETTER WORD ⊕																				

BINARY REPRESENTATION OF THE ALPHABET

A	0	0	0	0	0
B	0	0	0	0	1
C	0	0	0	1	0
D	0	0	0	1	1
E	0	0	1	0	0
F	0	0	1	0	1
G	0	0	1	1	0
H	0	0	1	1	1
I	0	1	0	0	0
J	0	1	0	0	1
K	0	1	0	1	0
L	0	1	0	1	1
M	0	1	1	0	0
N	0	1	1	0	1
O	0	1	1	1	0
P	0	1	1	1	1
Q	1	0	0	0	0
R	1	0	0	0	1
S	1	0	0	1	0
T	1	0	0	1	1
U	1	0	1	0	0
V	1	0	1	0	1
W	1	0	1	1	0
X	1	0	1	1	1
Y	1	1	0	0	0
Z	1	1	0	0	1

BINARY ADDITION TABLE

	0	1	0	1
+	0	+ 0	+ 1	+ 1
=	0	= 1	= 1	= 0

As long as Alice and Bob keep their shared key perfectly secret, there is no way for an eavesdropper to learn the message.

Note that sharing the key is different than sharing a message.

The key is a completely random binary sequence, and contains no useful information itself.

There is a risk of eavesdropper capturing the encryption key during the key distribution.

EXERCISE 4 (quantum encryption)

1. For each bit of the encryption key, Alice chooses the basis randomly (either + or ×)
2. Alice convert the bit and the basis into the photon polarization using the **BINARY-TO-POLARIZATION TABLE** given below.
3. Alice adjust the polarization rotator according to the polarization and sends polarized photons to Bob (Bob must be present to receive the key)

SECURE ENCRYPTION KEY
01000 11010 11011 00101

BINARY-TO-POLARIZATION TABLE

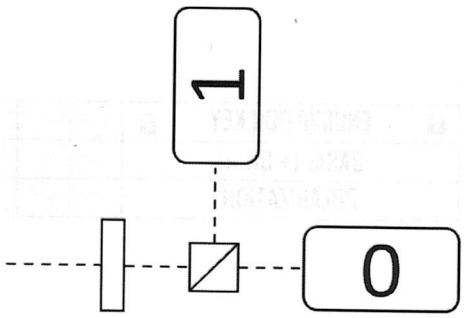
	BASIS +	BASIS ×
"0"	0°	-45°
"1"	90°	+45°

ENCRYPTION KEY																				
BASIS (+ OR ×)																				
POLARIZATION																				

EXERCISE 5
(receiving quantum encrypted message)

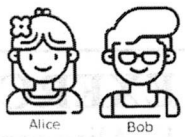
1. Before receiving each polarized photon from Alice, Bob randomly selects the basis and records in the table
2. Bob adjusts the polarization rotator for each chosen basis as either + (or 0°) or ×(+45°).
3. Using photodetectors, Bob receives the photon in the selected basis and records it as 0 or 1.
4. The process is repeated until all the encryption bits are received.

BASIS (+ OR ×)																			
RECEIVED BIT (0/1)																			

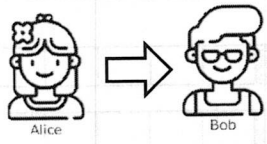


EXERCISE 6A (sharing bases)

1. Alice and Bob share bases



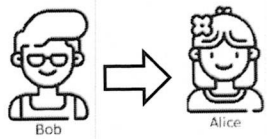
ALICE PUBLICLY SHARES HER BASIS CHOICE WITH BOB



ALICE'S BASIS CHOICE (to be given to Bob)

BASIS (+ OR ×)																			

BOB PUBLICLY SHARES HIS BASIS CHOICE WITH ALICE



BOB'S BASIS CHOICE (to be given to Alice)

BASIS (+ OR ×)																			

EXERCISE 6B (basis reconciliation)

1. Alice compares her basis choice with the basis choice received from Bob
2. Binary bits for different bases are discarded and binary bits for identical bases are kept.
3. Sifted encryption key (secure) is established (exchanged).

ALICE'S BASIS CHOICE FROM EXERCISE 4:

ENCRYPTION KEY																			
BASIS (+ OR ×)																			

BOB'S BASIS CHOICE FROM EXERCISE 6A:

BASIS (+ OR ×)																			
SIFTED KEY																			

EXERCISE 6C (basis reconciliation)

1. Bob compares his basis choice with the basis choice received from Alice
2. Binary bits for different bases are discarded and binary bits for identical bases are kept.
3. Sifted encryption key (secure) is established (exchanged).

ALICE'S BASIS CHOICE FROM EXERCISE 6A:

BASIS (+ OR ×)																			

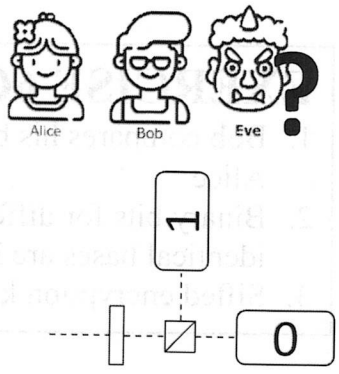
BOB'S BASIS CHOICE FROM EXERCISE 5:

BASIS (+ OR ×)																			
RECEIVED BIT (0/1)																			

SIFTED KEY																			

EXERCISE 7A (detecting Eve)

1. Repeat exercises 4 – 6.
2. For each qubit transfer, Eve records the photon and re-sends it to Bob
3. After they reconciled the bases, Alice and Bob perform spy test: compare certain number of bits from sifted key to see if any differences.
4. Can the presence of Eve be detected? Are there any discrepancies in the received versus sent bits in the spy test?



EXERCISE 4:

1. For each bit of the encryption key, Alice chooses the basis randomly (either + or ×)
2. Alice convert the bit and the basis into the photon polarization using the **BINARY-TO-POLARIZATION TABLE** given below.
3. Alice adjust the polarization rotator according to the polarization and sends polarized photons to Bob (Bob must be present to receive the key)

BINARY-TO-POLARIZATION TABLE

	BASIS +	BASIS ×
"0"	0°	-45°
"1"	90°	+45°

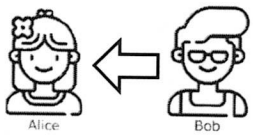
SECURE ENCRYPTION KEY
01000 11010 11011 00101

NOTE: CHOOSE BASIS FROM EXERCISE 4

ENCRYPTION KEY																				
BASIS (+ OR ×)																				
POLARIZATION																				

EXERCISE 6B:

4. Alice receives basis from Bob. She compares her basis choice with the basis choice received from Bob.
5. Binary bits for different bases are discarded and bits for identical bases are kept.
6. Sifted encryption key (secure) is established (exchanged).



ALICE'S BASIS CHOICE FROM EXERCISE 4:

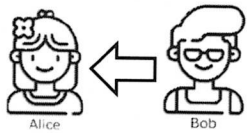
ENCRYPTION KEY																				
BASIS (+ OR ×)																				

BOB'S BASIS CHOICE FROM EXERCISE 5:

BASIS (+ OR ×)																				
SIFTED KEY (ALICE)																				

SPY TEST:

6. Receive sifted key from Bob
7. Any differences in Alice's versus Bob's sifted key?



SIFTED KEY (ALICE)																				

SIFTED KEY RECEIVED FROM BOB IN STEP 6:

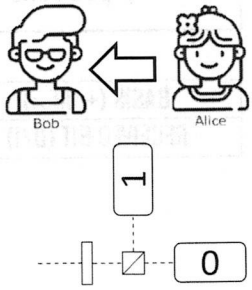
SIFTED KEY (BOB)																				

EXERCISE 7B (detecting Eve)

1. Repeat exercises 4 – 6.
2. For each qubit transfer, Eve records the photon and re-sends it to Bob
3. After they reconciled the bases, Alice and Bob perform spy test: compare certain number of bits from sifted key to see if any differences.
4. Can the presence of Eve be detected? Are there any discrepancies in the received versus sent bits in the spy test?

EXERCISE 5:

1. Before receiving each polarized photon from Alice, Bob randomly selects the basis and records in the table.
2. Bob adjusts the polarization rotator for each chosen basis as either + (or 0°) or ×(+45°).
3. Using photodetectors, Bob receives the photon in the selected basis and records it as 0 or 1.
4. The process is repeated until all the encryption bits are received.



NOTE: CHOOSE BASIS FROM EXERCISE 5

BASIS (+ OR ×)																		
RECEIVED BIT (0/1)																		

EXERCISE 6C:

5. Bob receives basis from Alice. He compares his basis choice with the basis choice received from Alice
6. Bits for different bases are discarded. Bits for identical bases are kept.
7. Sifted encryption key (secure) is established (exchanged).

ALICE'S BASIS CHOICE FROM EXERCISE 4:

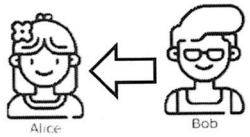
BASIS (+ OR ×)																		

BOB'S BASIS CHOICE FROM EXERCISE 5:

BASIS (+ OR ×)																		
RECEIVED BIT (0/1)																		
SIFTED KEY (BOB)																		

SPY TEST:

8. Receive sifted key from Bob
9. Any differences in Alice's versus Bob's sifted key?



SIFTED KEY (BOB)																		

SIFTED KEY RECEIVED FROM ALICE IN STEP 8:

SIFTED KEY (ALICE)																		

EXERCISE 7C
(receiving quantum encrypted message)

1. Before receiving each polarized photon from Alice, Eve randomly selects the basis and records in the table
2. Eve adjusts the polarization rotator for each chosen basis as either + (or 0^o) or ×($+45^o$).
3. Using photodetectors, Eve receives the photon in the selected basis and records it as 0 or 1.
4. Eve sends the bit she received to Bob.
5. The process is repeated until all the encryption bits are received.

BASIS (+ OR ×)																			
RECEIVED BIT (0/1)