COE817 – Lab 3

Jia fei Lin – 500782008

Key Distribution: Server Side

```
Received encrypted message1: b'$\x92\x08/,\x89\x05\xd4\xb5\xb6\xc6\x18\xddT\x8b\xea\x12[Z\x9f\xe7\x10\x1a5\xc6\xa7\x
92}J\xbd\x93\xe7\xd6\x92<J\xd8C\xf6\n@?CK\x16\xcbvH\t3{\xack\t"\xee\xbb\x12\x9c\xf14\x10K\xeb5\x8a\x0e\xf1\xf3\xa6\x
8e9\xf7$\xc4\xb7\r\xb1\xba,\xb0$\xd0\xe6\x94aa\xb8\x8b]\x99\x1f\x10.\xf9\x1c\\\x84\xef\x06\xe6\xd3`\xa7<\xc5\x94nu%\
x93\xc9:\x8e \xc0\xb5\xe0\xdf\x89\xa5\xcaD\xb0\x8f\xf0\x98\xd6'
Received message1: b'75267969INITIATOR A'
Received nonce1: 75267969
Message 2: 7526796903108993
Encrypted message2: b'\xc0\x8c\xfb\xd2\x18\xe6\xf6\xdb\xab\xb1p\xf5\x04/`\xca\xc58\xb9\xaeEFy%5\xee\x82a\xc7`B\xf0\x
a7%(h\x0b\xbeB%L\xd5\x91\x03!\xe5=\xf1\xee\xe2\xf0\x17\x13YGZ\x1bR\xf7z\x0eX\x18X\x82!I\xbf\x14t\xc3\xd7\x10\x03\xe1
\xf7\xf2=\x8a\xdds\xf3v\x96z\xf2\x8f\xcc^\x0f\xc7>\x8f\xc5\x1c\xbc\xf1g^\x06\xc2\xa6\x91\xc3\xc2\xfc\x87g.\x8d\x92L\
xf5\xee\x99B\xac\xeeH\xc8\xdf\xfd\x8e\x7f\x93\x89\xdd\xd3'
Received encrypted message3: b'\x0cS\xcfw\xdd-\xdb\xeb\xa0\xea^\xc0\x8eT!\xbf_^\x03\xf9E\xc27\xf1*?Y">\xac\x1a-\xc1\
x05\xe4l <\xb8\xad\xa5pm\xf0&!\x9et\x92*\xe2\x83\x95a,\x04\xf9\x98s\xe51\xbb\xd7\xbbV\xcfs\xebG_\xb5z3\xa9\xa9\x9c\x
e4e\x1e\x82\xc7t\xc0\x9a\xf7xG n\xfdj&\xc6\xf4\xe6\xa2\x0f|\x1f\x80\xbc\x1de\xf9\xe3\x9e\x03\xbd\xf9\x1c\xfb\x8ca[\x
e0_:G@i%]\x80\xb7=c\x04\x0c'
Received message3: b'03108993'
Received nonce2: 03108993
Received encrypted message4: b':8.\x1b\x0c\\\xaa\x19\x9f(\xdf\xd4m\xe02\xa5\x98u\xa7\xb3\xc0\x9f\xc4\x91\xf1\xca\xec
\xc3\xea\xdet^\x90\x0fK\x82\xdb.+\xc4\xf7.6\xc6\x112\xf48+?ID\xbch\x15U\x055\x03\xedK\x9f\xe3FT\x01\xc8\xfd9i\xed\xb
d\xdc\x8e\x92.\xbaNO\xc9FF\x7f"~B\xc3\x15\x9c01\xd8\xcbVV\x13\xce;\x7f\xa0\xaee\xc9r\xad\xdb\xc2M^9\x99\xc2\x96\x10,
\xa3\xc1Z\xf4\xa0\x82\xb2\x89}\xf6h\xfd~'
Received session key: b'\xb6c[)\x81\xdf\xc0\xd9'
```

Key Distribution: Client Side

```
Message1: 75267969INITIATOR A
Encrypted message1: b'$\x92\x08/,\x89\x05\xd4\xb5\xb6\xc6\x18\xddT\x8b\xea\x12[Z\x9f\xe7\x10\x1a5\xc6\xa7\x92}J\xbd\
x93\xe7\xd6\x92<J\xd8C\xf6\n@?CK\x16\xcbvH\t3{\xack\t"\xee\xbb\x12\x9c\xf14\x10K\xeb5\x8a\x0e\xf1\xf3\xa6\x8e9\xf7$\
xc4\xb7\r\xb1\xba,\xb0$\xd0\xe6\x94aa\xb8\x8b]\x99\x1f\x10.\xf9\x1c\\\x84\xef\x06\xe6\xd3`\xa7<\xc5\x94nu%\x93\xc9:\
x8e \xc0\xb5\xe0\xdf\x89\xa5\xcaD\xb0\x8f\xf0\x98\xd6'
Received encrypted message2: b'\xc0\x8c\xfb\xd2\x18\xe6\xf6\xdb\xab\xb1p\xf5\x04/`\xca\xc58\xb9\xaeEFy%5\xee\x82a\xc
7`B\xf0\xa7%(h\x0b\xbeB%L\xd5\x91\x03!\xe5=\xf1\xee\xe2\xf0\x17\x13YGZ\x1bR\xf7z\x0eX\x18X\x82!I\xbf\x14t\xc3\xd7\x1
0\x03\xe1\xf7\xf2=\x8a\xdds\xf3v\x96z\xf2\x8f\xcc^\x0f\xc7>\x8f\xc5\x1c\xbc\xf1g^\x06\xc2\xa6\x91\xc3\xc2\xfc\x87g.\
x8d\x92L\xf5\xee\x99B\xac\xeeH\xc8\xdf\xfd\x8e\x7f\x93\x89\xdd\xd3'
Received message2: b'7526796903108993'
Received nonce2: b'03108993'
Message3: b'03108993'
Encrypted message3: b'\x0cS\xcfw\xdd-\xdb\xeb\xa0\xea^\xc0\x8eT!\xbf_^\x03\xf9E\xc27\xf1*?Y">\xac\x1a-\xc1\x05\xe4l
<\xb8\xad\xa5pm\xf0&!\x9et\x92*\xe2\x83\x95a,\x04\xf9\x98s\xe51\xbb\xd7\xbbV\xcfs\xebG_\xb5z3\xa9\xa9\x9c\xe4e\x1e\x
82\xc7t\xc0\x9a\xf7xG n\xfdj&\xc6\xf4\xe6\xa2\x0f|\x1f\x80\xbc\x1de\xf9\xe3\x9e\x03\xbd\xf9\x1c\xfb\x8ca[\xe0_:G@i%]
\x80\xb7=c\x04\x0c'
Session Key: b'\xb6c[)\x81\xdf\xc0\xd9'
Encrypted message4: b':8.\x1b\x0c\\\xaa\x19\x9f(\xdf\xd4m\xe02\xa5\x98u\xa7\xb3\xc0\x9f\xc4\x91\xf1\xca\xec\xc3\xea\
xdet^\x90\x0fK\x82\xdb.+\xc4\xf7.6\xc6\x112\xf48+?ID\xbch\x15U\x055\x03\xedK\x9f\xe3FT\x01\xc8\xfd9i\xed\xbd\xdc\x8e
\x92.\xbaNO\xc9FF\x7f"~B\xc3\x15\x9c01\xd8\xcbVV\x13\xce;\x7f\xa0\xaee\xc9r\xad\xdb\xc2M^9\x99\xc2\x96\x10,\xa3\xc1Z
\xf4\xa0\x82\xb2\x89}\xf6h\xfd~'
```

COE817 – Lab 3

Jia fei Lin – 500782008

Messaging Application: Server Side

```
b'Secure Communication Channel Authenticated.'
Please enter a message to encrypt and send to the server(to exit enter 0):
hello world
Encrypted Message: b"\x14%s\x15\xefj\x1a\x16\x01)\xdf\x01G'hjC\x99\x05"
Please enter a message to encrypt and send to the server(to exit enter 0):
Thank you for another 100
Encrypted Message: b'<\x85-$\xc4?Rk\x18\xf3BM\xf1\xbe}L?\xbag\t\x1cD\x0c0_\x1b\x8aB\xfbw;\xa0\x96\x85'
Please enter a message to encrypt and send to the server(to exit enter 0):
Have a nice day, evening
Encrypted Message: b'\xe2\xe1X\xbe\x1f\xad\xbcq\x82\xd8\xf3\x86\x9f\xc2w\xba\xf7&X\x91~\x9e]Hr\r0\t\xa8p\xa3\x03'
Please enter a message to encrypt and send to the server(to exit enter 0):
0
Encrypted Message: b'7\x05 1\xd2\xd6\xa2^c'
```

Messaging Application Client Side

```
Messaging Application:
Received encrypted message: b"\x14%s\x15\xefj\x1a\x16\x01)\xdf\x01G'hjC\x99\x05"
Client sent: b'hello world'
Received encrypted message: b'<\x85-$\xc4?Rk\x18\xf3BM\xf1\xbe}L?\xbag\t\x1cD\x0c0_\x1b\x8aB\xfbw;\xa0\x96\x85'
Client sent: b'Thank you for another 100 '
Received encrypted message: b'\xe2\xe1X\xbe\x1f\xad\xbcq\x82\xd8\xf3\x86\x9f\xc2w\xba\xf7&X\x91~\x9e]Hr\r0\t\xa8p\xa
3\x03'
Client sent: b'Have a nice day, evening'
Received encrypted message: b'7\x05 1\xd2\xd6\xa2^c'
Client sent: b'0'
```

How to prevent replay attacks:

Replay attacks occur when a cybercriminal intercepts communication on secure networks and then delays or resends information to fulfill the hacker's goals. In order to stop such attacks, the right method of encryption must be used. Some methods include:

1. Both sender and receiver should create a random session key to be used only for a single transaction
2. Both sender and receiver use timestamps during their exchanges to mark exactly when messages were sent.
3. Utilize a password for each transaction that will be used and discarded. This makes it such that even if the attacker has the message and sends it, the encryption password would already be expired and no longer works.