FIT9137 Applied Week 11

Topics:

- Network Security
  - Symmetric Key Cryptography
  - Asymmetric Key Cryptography (AKA - Public Key Cryptography)

Covered Learning Outcomes:

- identify and describe fundamental concepts of network security mechanisms against common threats and countermeasures.

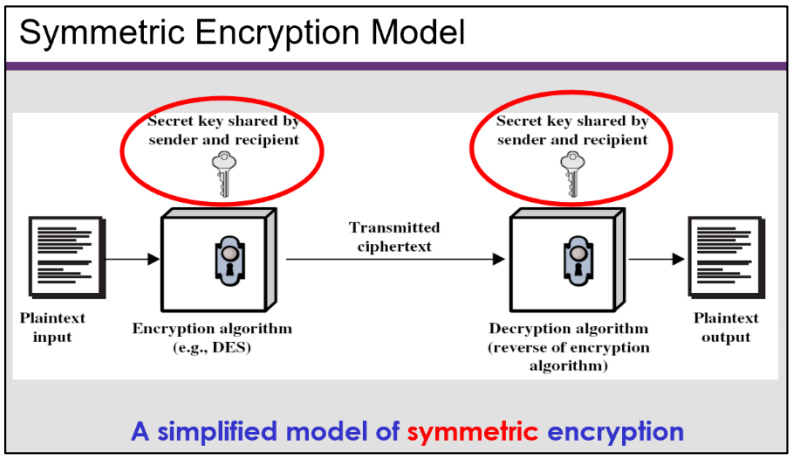
Instructions

- One of the main purposes of an applied session is to build the learning community, create connections and include the learners. The other goal is to give and receive feedback from your peers and or your tutors.
- Form groups of 2 students (online) or more for face-to-face to work through the exercises. If met a problem, try to solve it by asking direct questions to your peer. If the issue was not solved within peers, ask your tutor. If did not get a chance to solve the problem during your applied session with your peer or tutor, jump into one of many consultation hours and ask any of the tutors to help you. Please visit the "Teaching Team and Unit Resources" tile in the FIT9137 Moodle site.

Network Security

I. Symmetric Key Cryptography

Symmetric-key algorithm is algorithm for cryptography that use the same cryptographic keys for both the encryption of plaintext and the decryption of ciphertext. The keys are identical. The key, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. The requirement that both parties should have access to the secret key in a secure manner is one of the main challenges of symmetric-key encryption. (https://en.wikipedia.org/wiki/Symmetric-key_algorithm).



We will use the page Cryptography Lab[1] for this exercise. The following steps are performed using the **symmetric encryption** links.

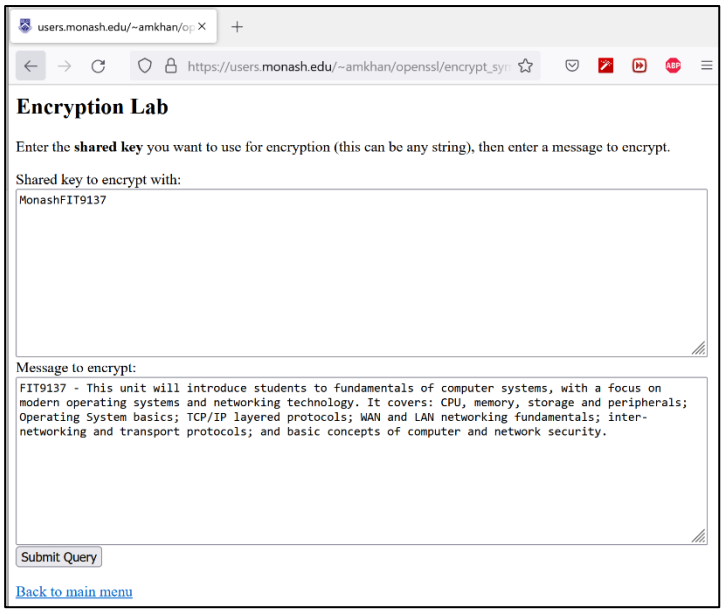
[1]https://users.monash.edu/~amkhan/openssl/index.html

STEP 1. Confidentiality

In this exercise we will learn how to send a confidential message using Symmetric Key encryption algorithm. Ask a fellow student to form a group with you to complete this exercise.

STEP 2. Generating a Symmetric Key Pair

In Cryptography Lab page click on the link *Encrypt a message with a shared key*. You should see a page as follows:



Note that the Symmetric Key selected is a shared key between the two users is "`MonashFIT9137`".

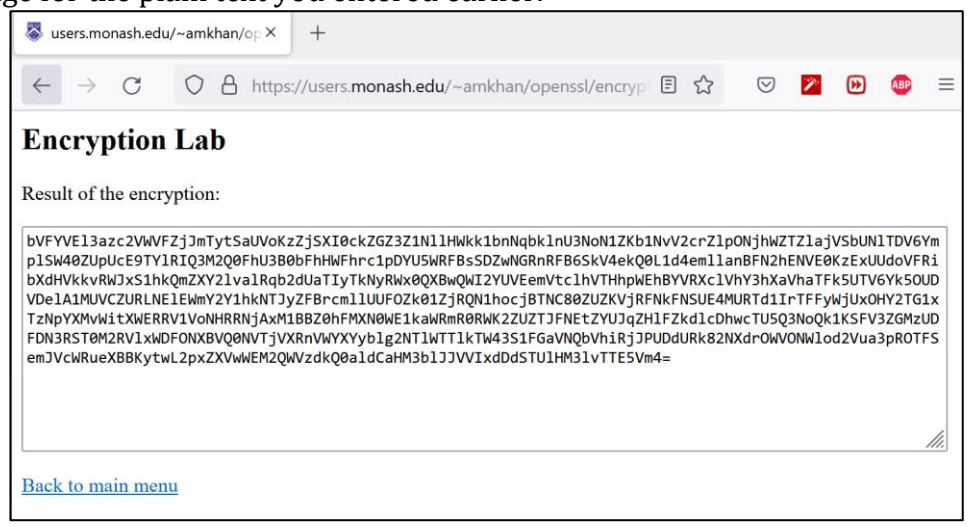
STEP 3. Key Exchange

Please Share the shared **Symmetric key** with your group mate.

STEP 4. Confidential Message

1. Once you submit the Query, you will get the encrypted data as follows: -

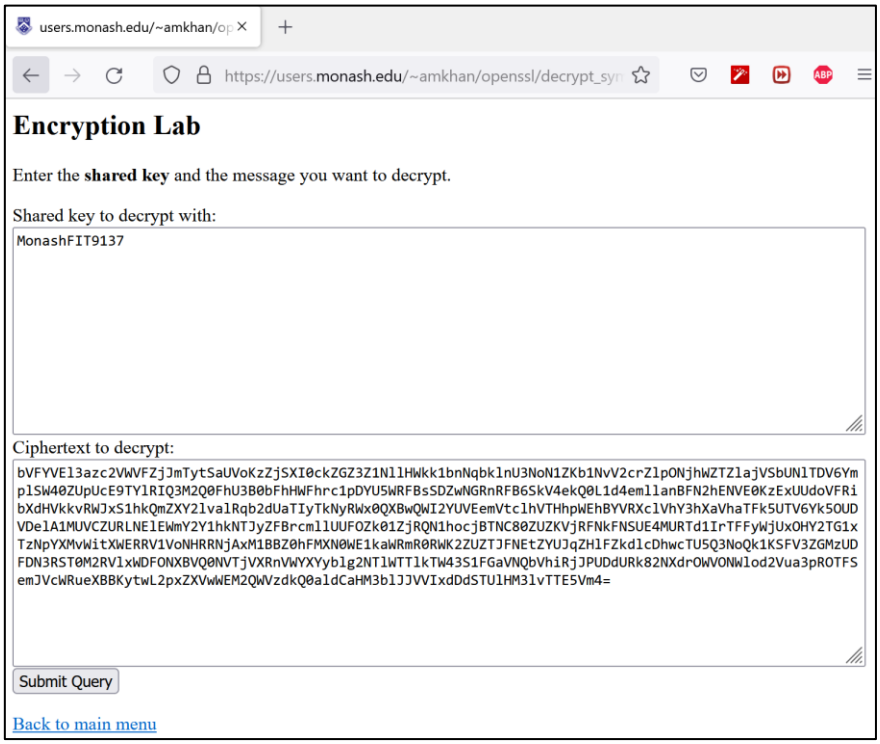
STEP 5. Clicking on the Submit Query button, would have generated the encrypted message for the plain text you entered earlier.



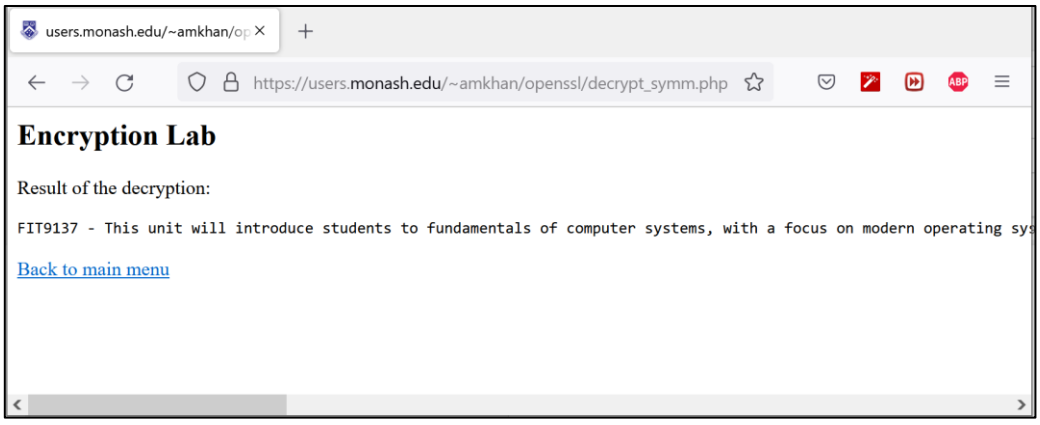
STEP 6. Send the ciphertext to your group mate. Your group mate should send you an encrypted message as well using the shared Symmetric key "`MonashFIT9137`".

STEP 7. **From** the main page of Cryptography Lab click the link *Decrypt a message with a shared key*. Copy and paste the encrypted message and your shared

Symmetric key in the corresponding fields and decrypt the message from your group mate.

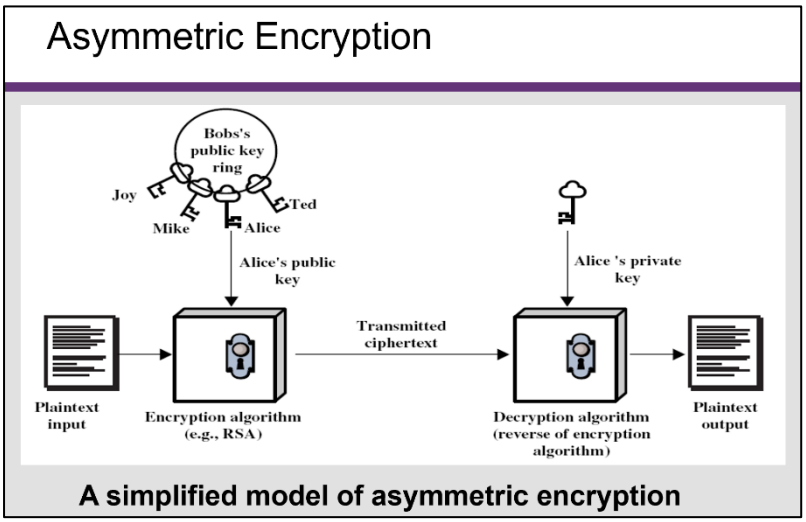


STEP 8. Clicking on the Submit Query button, would have generated the original message for the cipher text you received earlier.



II. Public Key Cryptography

Public-key cryptography, or asymmetric cryptography, is a cryptographic system that uses pairs of keys. Each pair consists of a public key (which is shared and known to others) and a private key (which is not shared or known by anyone except the owner). The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions. Effective security requires keeping the private key private; the public key can be openly distributed without compromising security. (https://en.wikipedia.org/wiki/Public-key_cryptography)



We will use the page Cryptography Lab[2] for this exercise. The following steps are performed using the **Asymmetric encryption** links.

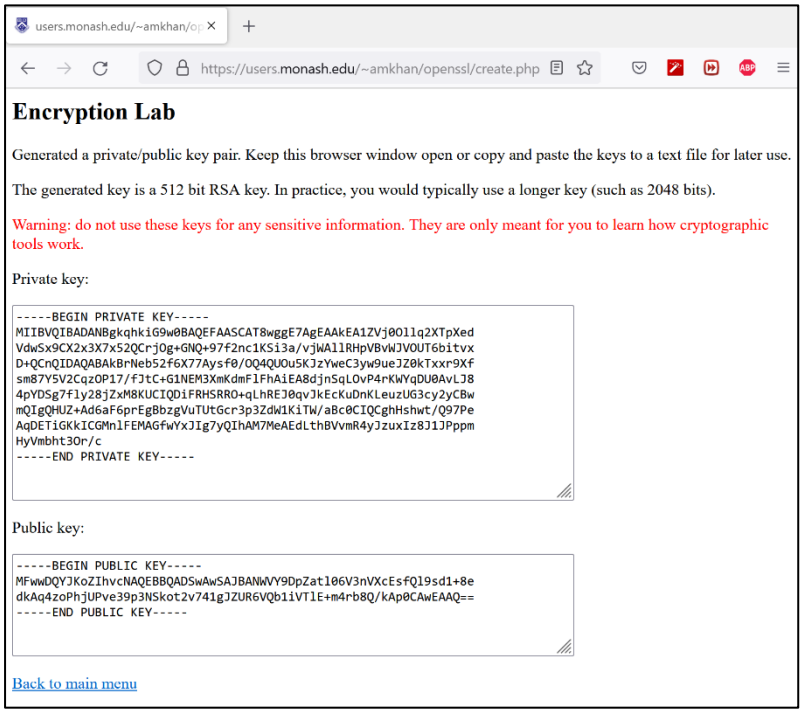
STEP 1. 1.1 Confidentiality

In this exercise we will learn how to send a confidential message using RSA public key algorithm. Ask a fellow student to form a group with you to complete this exercise.

STEP 2. 1.1.1 Generating a Key Pair

In Cryptography Lab page click on the link *Create new private/public key pair*. You should see a page as follows (different values for Public and Private keys):

Keep this page open or copy both keys into a text file and save.



Generating Key Pair using Cryptography Lab Page

[2] https://users.monash.edu/~amkhan/openssl/index.html

STEP 3. **1.1.2 Key Exchange**

Share your **public key** with your group mate.

Confidential Message

STEP 4. From the main page of Cryptography Lab click the link *Encrypt a message using a public key* (open in a new tab or page) and use the public key of your group mate (recipient) and encrypt a message. Click on the Submit Query button once you are done entering the message.

STEP 5. Send the ciphertext to your group mate. Your group mate should send you an encrypted message as well using your public key.

STEP 6. From the main page of Cryptography Lab click the link *Decrypt a message using a private key*. Copy and paste the encrypted message and your private key to the corresponding fields and decrypt the message from your group mate.

III. Digital Signature

STEP 1. From the main page of Cryptography Lab click the link *Sign a message using a private key*.

STEP 2. You as the sender must use your private key to sign a message. Create a message and send it along with generated digital signature to your group mate (exchange messages).

STEP 3. From the main page of Cryptography Lab click the link *Verify a signature using a public key*. Use the received message, its digital signature, and the public key of your group mate (sender) to verify that the message is authentic.

STEP 4. Make a small change in the message and repeat step 3. Is the signature valid for the changed message?