

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.

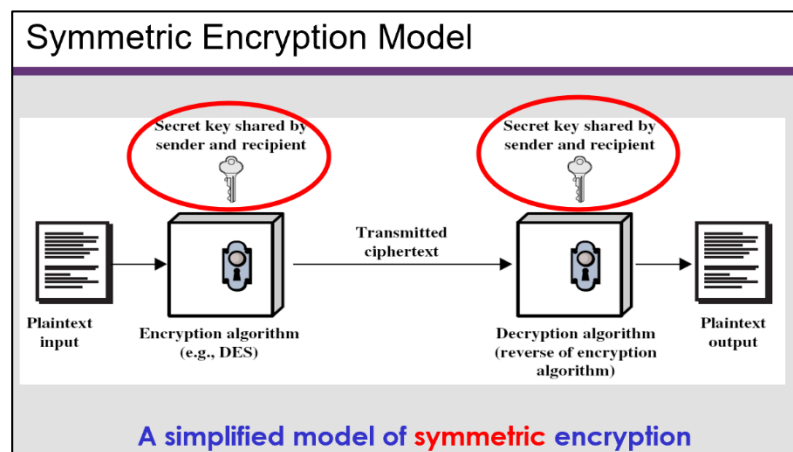
Network Security

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:

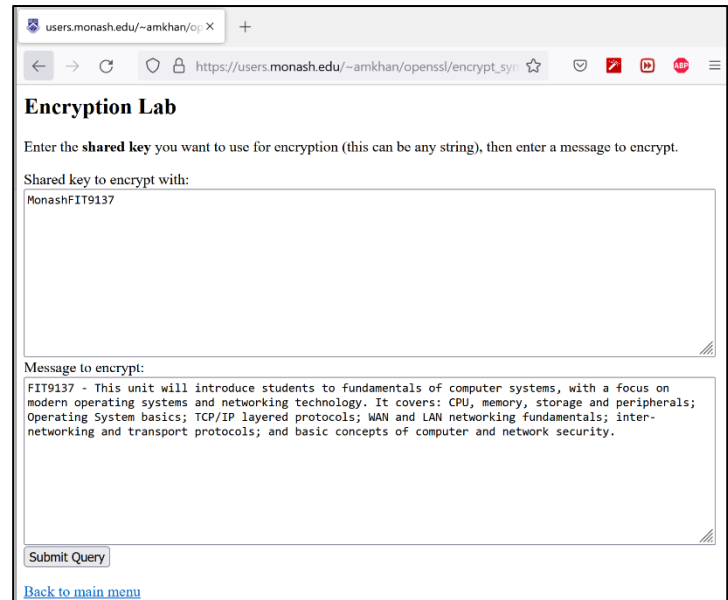
Note that the Symmetric Key selected is a shared key between the two users is "MonashFIT9137".

STEP 3. Key Exchange

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

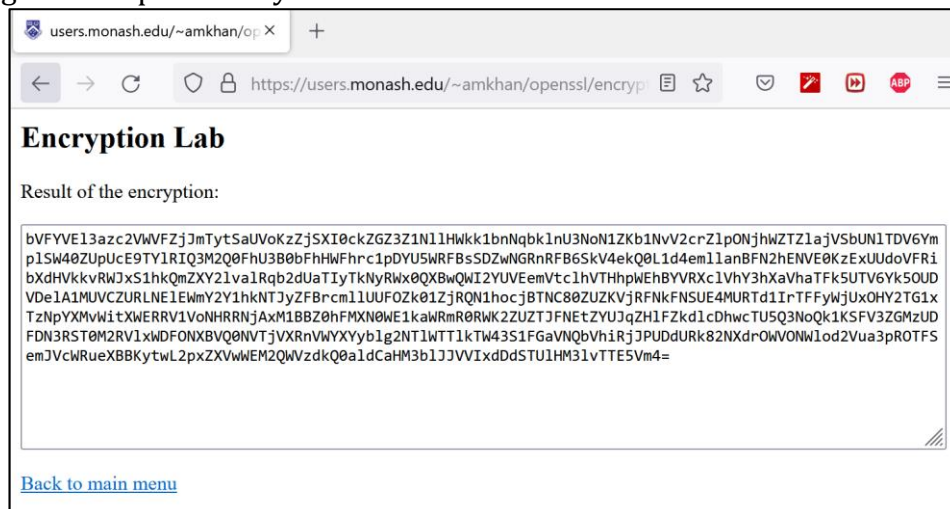
STEP 4. Confidential Message

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



The screenshot shows a web browser window with the URL https://users.monash.edu/~amkhan/openssl/encrypt_sy. The page is titled "Encryption Lab". It contains two text input fields. The first field is labeled "Shared key to encrypt with:" and contains the text "MonashFIT9137". The second field is labeled "Message to encrypt:" and contains the text "FIT9137 - This unit will introduce students to fundamentals of computer systems, with a focus on modern operating systems and networking technology. It covers: CPU, memory, storage and peripherals; Operating System basics; TCP/IP layered protocols; WAN and LAN networking fundamentals; inter-networking and transport protocols; and basic concepts of computer and network security." Below the input fields is a "Submit Query" button and a "Back to main menu" link.

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

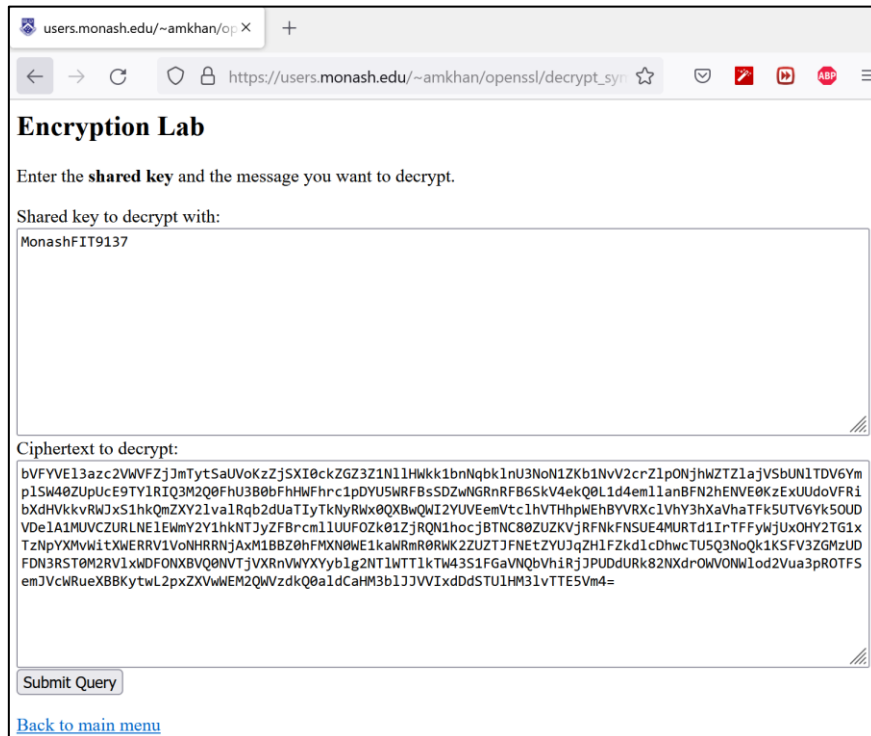


The screenshot shows the same web browser window as before, but the "Result of the encryption:" section now displays a long string of encrypted data: "bVFYVE13azc2VwVFZjJmTyTtSaUvoKzZjSXI0ckZGZ3Z1N1lHwkk1bnNqbklN1U3NoN1ZKb1NvV2crZ1pONjhWZT1a1jVSbUN1TDV6Ym p1SW40ZUpUcE9TY1RIQ3M2Q0FhU3B0bFhHWFhrc1pDYU5WRFBsSDZwNGRnRFB6SkV4ekQ0L1d4em1lanBFN2hENVE0KzExUUdoVFRi bXdHvkvRWJxS1hkQmZXY21va1Rqb2dUaTiyTkNyRwx0QXBwQW12YUVEemVtc1hVTHhpWheBYVRxc1VhY3hXaVhaTFk5UTV6Yk50UD VDe1A1MUVVCZURLNE1EwmY2Y1hkNTJyZFBrcm1lUUF0Zk01ZjRQNi1h0c1BTNC80ZUZKvJRfNkFNSUE4MURtd1IrTFFYwJjUx0HY2TG1x TzNpYXNvWitXWERRV1VoNHRNjAxM1BBZ0hFMXN0WE1kawRmR0RwK2ZUZTJFNEtZYUJqZHI1FZkd1cDhwcTU5Q3NoQk1KSFV3ZGMzUD FDN3RST0M2RV1xwDFONXBVQ0NVtjVXRnVWYXYyb1g2NT1WTT1kTW43S1FGaVNBQbVh1rjJPUDdURk82NXdrOWVONWlod2Vua3pROTFS emJvcWRueXBBKytWl2pxZXVwWEM2QWVzdkQ0a1dCaHM3b1JJVV1xdDdStU1HM31vTTE5Vm4=".

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.



The screenshot shows a web browser window with the URL `https://users.monash.edu/~amkhan/openssl/decrypt_symm.php`. The page is titled "Encryption Lab". It contains two input fields: "Shared key to decrypt with:" and "Ciphertext to decrypt:". The shared key field contains the text "MonashFIT9137". The ciphertext field contains a long, multi-line string of base64-encoded data. Below the ciphertext field is a "Submit Query" button and a link "Back to main menu".

users.monash.edu/~amkhan/op: X +

← → ↻ 🔒 https://users.monash.edu/~amkhan/openssl/decrypt_symm.php ☆ 📧 📺 📺 📺 📺

Encryption Lab

Enter the **shared key** and the message you want to decrypt.

Shared key to decrypt with:

MonashFIT9137

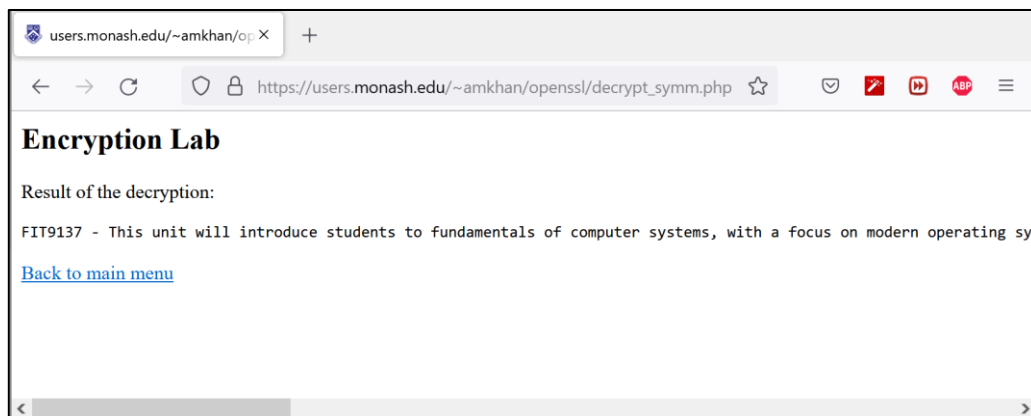
Ciphertext to decrypt:

bVFYVE13azc2VWVFZjJmTytSaUvoKzZjSXl0ckZGZ3Z1NlHwkk1bnNqbklNlU3NoN1ZKb1NvV2crZ1pONjhWZTl1aJVSbUN1TDV6Ym
p1S4W0ZUpUceF9TY1RIQ3M2Q0FhU3B0bFhHwFhrc1pDYU5WRFBSsSDZwNGRnRFB6SkV4ekQ0L1d4em1lanBFN2hENVE0KzExUudoVFR1
bXdHvKkRwJxS1hkQmZXY21va1Rqb2dUaTiYtKNyRwX0QBwQWI2YUVEemVtc1hVTHhpWWhBYVRxc1VhY3hXaVhaTFk5UTV6Yk5OUJ
VDe1A1MUVcZURLNE1Ewmy2Y1hKNTJyZFBrcm1lUUF0Zk0IZjRQNIhocjBTNC80ZUZKvJRFNkFNSUE4MURtd1IrTFFyWjUxOHY2TG1x
TzNpYXNvVWltXWERRV1VoNHRnRnJAxM1BBZ0hFMXN0WE1kaWRmR0R0Wk2ZUZTJFNEtZYUJqZHI1FZkd1cDhwcTU5Q3NoQk1KSfV3ZGMzUD
FDN3RST0M2RV1xwDFONXBVQ0NVTjVXRnVWYXYyb1g2NTlWTTlkTW43S1FGaVnQbVh1RjJPUddURk82NXdrOWVONW1od2Vua3pROTFS
emJVCwRueXBBKytWl2pxZXVwWEM2QWVzdkQ0a1dCaHM3b1JJVVIxdDdStU1HM31vTTE5Vm4=

Submit Query

[Back to main menu](#)

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



The screenshot shows the same web browser window after clicking the "Submit Query" button. The page now displays the "Result of the decryption:" section, which shows the text "FIT9137 - This unit will introduce students to fundamentals of computer systems, with a focus on modern operating systems". Below this text is a link "Back to main menu".

users.monash.edu/~amkhan/op: X +

← → ↻ 🔒 https://users.monash.edu/~amkhan/openssl/decrypt_symm.php ☆ 📧 📺 📺 📺 📺

Encryption Lab

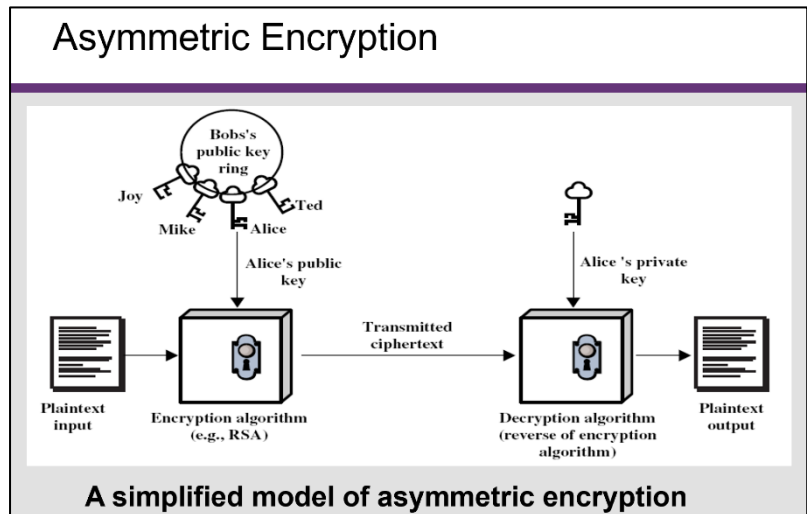
Result of the decryption:

FIT9137 - This unit will introduce students to fundamentals of computer systems, with a focus on modern operating systems

[Back to main menu](#)

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](https://users.monash.edu/~amkhan/openssl/create.php)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](https://users.monash.edu/~amkhan/openssl/create.php) 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*

users.monash.edu/~amkhan/o/ x +

← → ↻ 🔒 https://users.monash.edu/~amkhan/openssl/create.php

Encryption Lab

Generated a private/public key pair. Keep this browser window open or copy and paste the keys to a text file for later use.

The generated key is a 512 bit RSA key. In practice, you would typically use a longer key (such as 2048 bits).

Warning: do not use these keys for any sensitive information. They are only meant for you to learn how cryptographic tools work.

Private key:

```
-----BEGIN PRIVATE KEY-----
MIIBVQIBADANBgkqhkiG9w0BAQEFAASCAT8wggE7AgEAAkEA1ZVj0011q2XTpXed
Vdws9XC2x3X7x52QCr-j0g+GNQ+97F2nc1KS13a/vjWA11RHpVBvWJVOUT6bitvx
D+QcNqIDAQABAkBrNeb52f6X77Aysf0/OQ4QU0u5KJzYweC3yw9ueJZ0kTxr9XF
sm87Y5V2CqzOP17/FJtC+G1NEM3XmKdmF1FhA1EA8dJnSqL0vP4+KwYqDU0AvLJ8
4pYDSg7f1y28jZxM8KUCIQD1FRHSRR0+qLhREJ0qvJkEcKuDnKLeuzUG3cy2yCBw
mQIGQHUZ+Ad6aF6prEgBbzgVuTUtgcr3p3Zdw1K1TW/aBc0CIQCghHshwt/Q97Pe
AqDEt1GKk1CGMn1FEMAGfwYxjIgf7yQIhAM7MeAEdLthBVmR4yJzux1z8J1JPppm
HyVmbht30r/c
-----END PRIVATE KEY-----
```

Public key:

```
-----BEGIN PUBLIC KEY-----
MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANWVY9DpZat106V3nVXcEsFQ19sd1+8e
dkAq4zoPhjUPve39p3NSkot2v741gJZUR6VQb11VT1E+m4rb8Q/kAp0CAwEAAQ==
-----END PUBLIC KEY-----
```

[Back to main menu](#)

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?