# FIT1047 Applied Session Week 10

# CYBERSECURITY BASICS

## OBJECTIVES

- The purpose of this applied session is getting to know (i) different types of cryptography and (ii) data movements in Virtual Private Networks (VPN).

## INSTRUCTIONS

- For some of the questions, you may have to refer to the pre-class video and associated slides available in the Moodle.
- You may work in a small group.

## Activity 1: Learn about Monoalphabetic Substitution via Cryptool Online

In this task we get to know Cryptool, a learning tool for cryptography. We use the online version at https://www.cryptool.org/en/. This version mainly supports classical ciphers up to after the Second World War. Ciphers can directly be tested. However, as the interface is a bit clumsy for the task of guessing a key, we use a small tool in the Moodle at "FIT1047 Unit Resources" section.

For learning about modern cryptography, the full version of the tool for Windows can be downloaded here: https://www.cryptool.org/
a) Load Cryptool online at "https://www.cryptool.org/en/cto/"
b) Choose the Monoalphabetic Substitution Cipher from the Ciphers Menu. Choose "Description" and read the text on the Monoalphabetic substitution cipher.
c) Read the descriptions for the Caesar cipher and the Vigen'ere cipher. Why can the Vigen'ere cipher be considered more secure? Why is it still a very insecure cipher if the key-length is not long enough? (Hint: Read the Security sections).

## Sample Solution:

https://www.cryptool.org/en/cto-ciphers/caesar
https://www.cryptool.org/en/cto-ciphers/monoalpha
https://www.cryptool.org/en/cto-ciphers/vigenere

While the Caesar cipher just shifts the alphabet, the Vigen'ere cipher uses a key to choose between different shifts of the alphabet. Nevertheless, if the length of the key is known, it is still possible to do a frequency analysis. It can be made secure by using a random sequence of characters for the key and it is unbreakable.

# Activity 2: Monoalphabetic Substitution Cipher: Decryption exercise

The following ciphertext is derived from an English plaintext using a Monoalphabetic Substitution Cipher. It is not case sensitive, punctuation is unencrypted, and blanks are not deleted. Use the tool under Unit Information Monoalphabetic Substitution Tool in Moodle.

You should see the screen shown here:

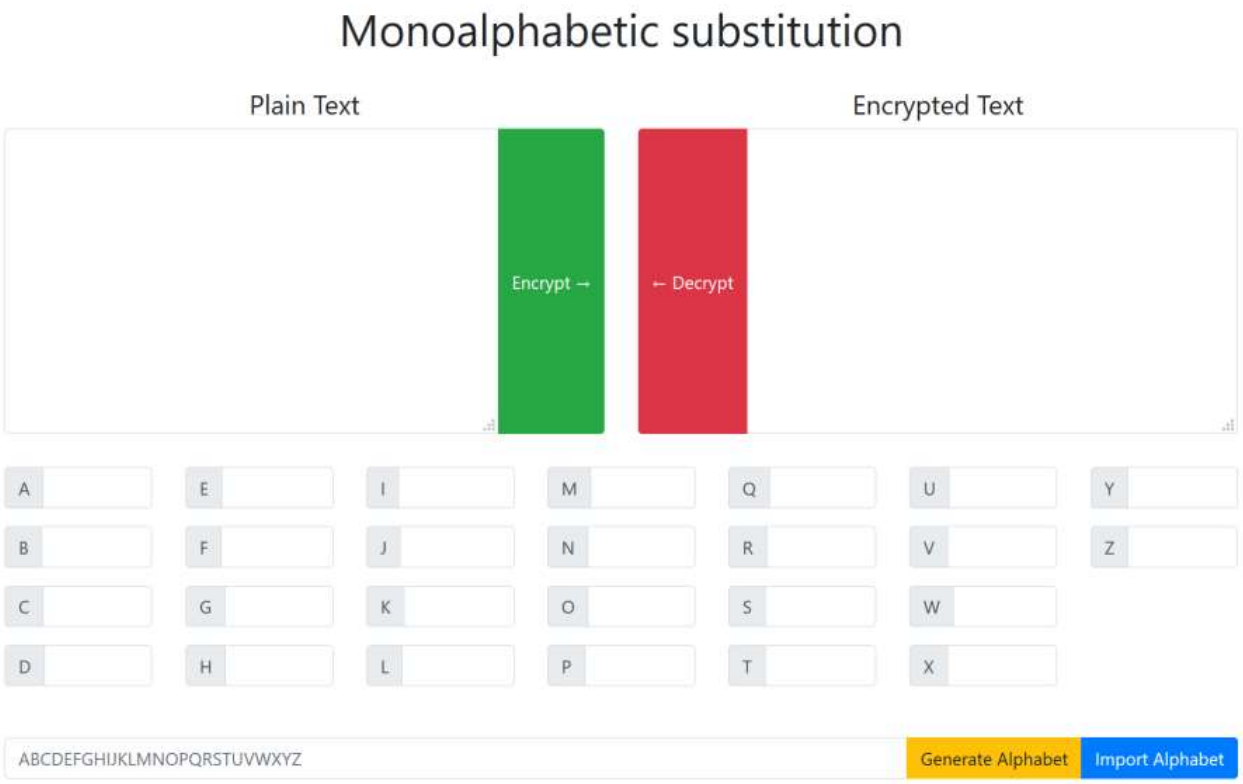


Figure 1: Monoalphabetic Substitution

**A few hints before you start:**

(a) Copy the ciphertext into the Encrypted Text.
(b) Note that while the encrypted text might contain lower case and symbols, the plaintext will be in upper case.
(c) Now start trying letters. E.g. if you think a ciphertext g should become a plaintext P, just write g into the box next to P.
(d) Next, you can click Decrypt and the plaintext in accordance with your guess of the key will appear in the Plain Text box.

- Caution: Clicking Encrypt will overwrite the text in the Encrypted Text box.

‘f9y2 x$m fnay mg q2 d9y u$s2q2k, g$$9,‘
jnqc gqkwyd nd wnjd,
‘f9nd qj d9y 6qsjd d9q2k x$m jnx d$ x$msjyw6?‘

‘f9nd qj 6$s rsyna6njd?‘ jnqc g$$9.
‘f9nd c$ x$m jnx, gqkwyd?‘

‘q jnx, q f$2cys f9nd qj k$q2k d$ 9nggy2 ybtqdq2k d$cnx?‘ jnqc gqkwyd.
g$$9 2$ccyc d9$mk9d6mwwx. ‘qd qj d9y jnuy d9q2k,‘ 9y jnqc.

Try to answer the following questions:
a) Which approach would you choose to start an analysis of this ciphertext?
b) What is the plaintext?

c) Which key is used?

## Sample Solution:

Answer:

a) First count letters and look at the frequency. Then, try short words (2 letter words) and then look for structure, e.g. words that appear very often.

b) The plaintext is a quote from A.A. Milne‘s book “Winnie the Pooh”:

‘When you wake up in the morning, Pooh,‘
said Piglet at last,
‘What is the first thing you say to yourself?‘
‘What is for breakfast?‘ said Pooh.
‘What do you say, Piglet?‘
‘I say, I wonder what is going to happen exciting today?‘ said Piglet.
Pooh nodded thoughtfully. ‘It is the same thing,‘ he said.

c) The key is:

nrtcy6k9qJawu2$gQsjdmVfbxZ

## Activity 3: Examine VPNs Using Captured Packets using Wireshark

This activity contains a simulated network consisting of a private network on the right, Internet (represented by some interconnected routers) in the middle, and a client PC on the left. The client PC runs a vpn client application that wants to connect to the vpn server in order to access the private network (subnet address 10.0.6.0/24).

The vpn client application is configured to communicate with the vpn server (IP Address: 10.0.6.1/24) to get its IP address (from vpn-subnet 10.0.200.0/24) in order for the vpn client to be a part of the vpn subnet. Here, the vpn server facilitates packet movement between the vpn subnet and the private network.

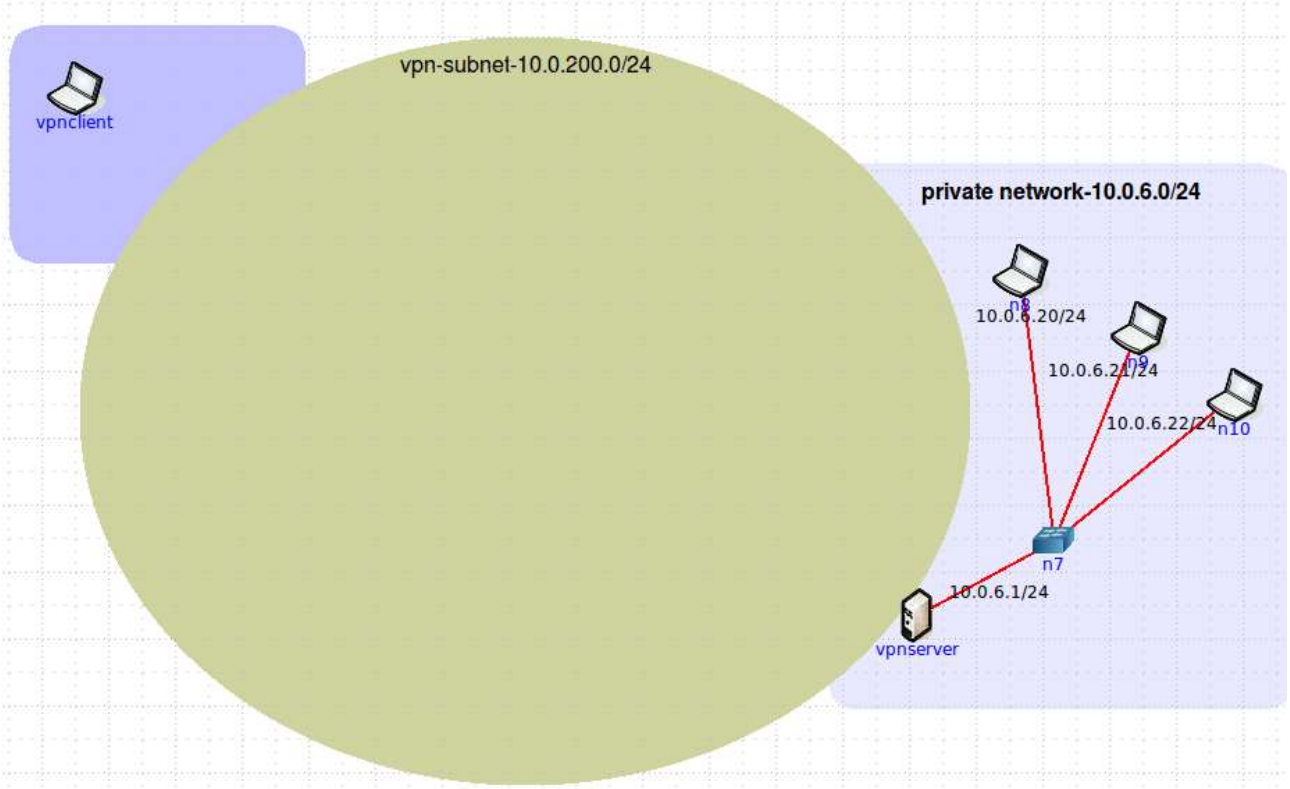


Figure 2: A VPN Subnet and a private network

The PC hosting the vpn client is part of the subnet 10.0.0.0/24 which is connected to the Internet. The vpn client will prepare IP datagrams (vpn client Source IP: 10.0.200.X, private network Destination IP: 10.0.6.20) encrypt them before encapsulating using public IP addresses (Source IP: 10.0.0.20, Destination IP: 10.0.1.10).

We captured packets in two locations (in the client subnet and inside the private network) while running a ping command at the client PC to reach node n8 in the private network. The file “FIT1047-2022-Applied-W10-Q3**a**.pcapng” contains packets captured in the client subnet and the file “FIT1047-2022-Applied-W10-Q3**b**.pcapng” contains packets captured in the private network.

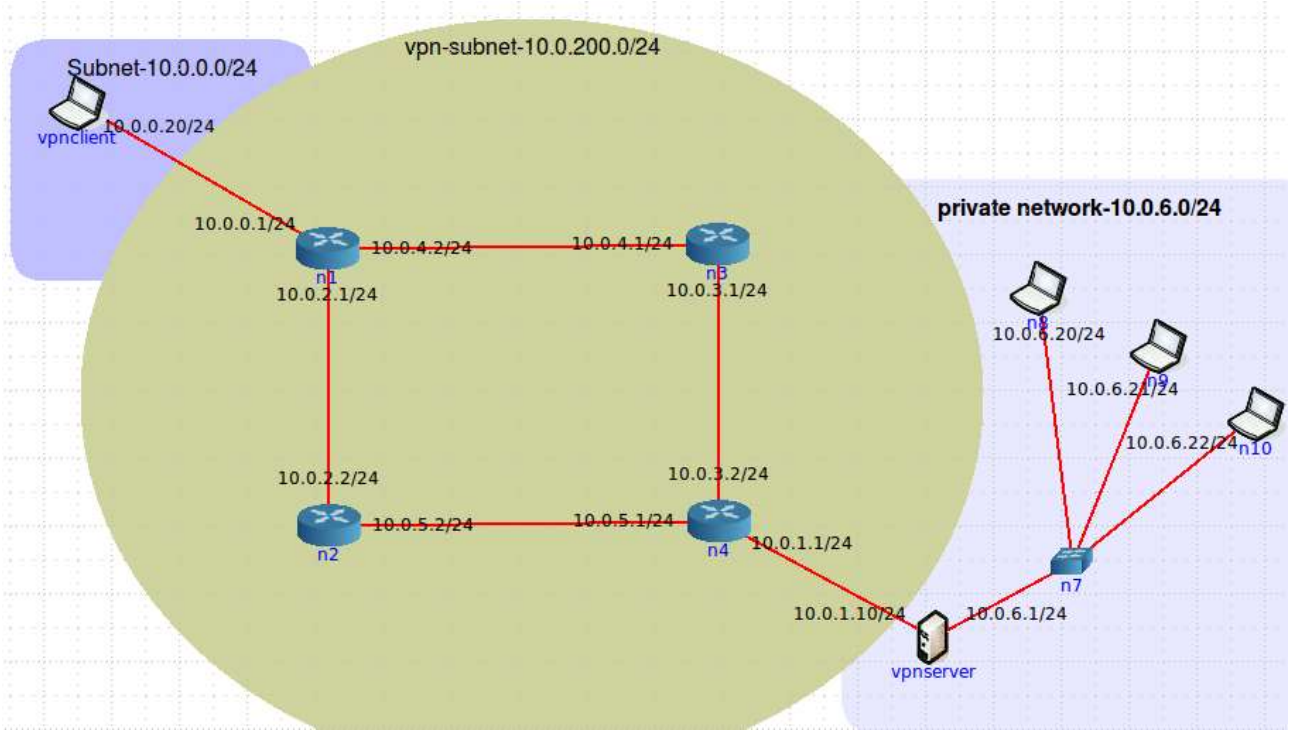


Figure 3: A VPN Subnet, a private network and the connecting network

(i) Analyze the frame 1 captured in “FIT1047-2022-Applied-W10-Q3**a**.pcapng” and answer the following questions.

(a) What are the source and destination IP addresses used in the packets captured? Does it match your expectations?

(b) Can you see the data contents? Which device will decapsulate this IP datagram and decrypt this data?

(ii) Analyze the frame 1 captured in “FIT1047-2022-Applied-W10-Q3**b**.pcapng” and answer the following questions.

(a) What are the source and destination IP addresses used in the packets captured? Which device has inserted these IP datagrams in the private network?

(b) Can you see the data contents? Which device created this IP datagram contents?

Solution:

(i) Analyze the frame 1 captured in “FIT1047-2022-Applied-W9-Q3a.pcapng” and answer the following questions.

(a) What are the source and destination IP addresses used in the packets captured? Does it match your expectations?

IP-Source: 10.0.0.20, IP- Destination: 10.0.1.10

The source IP is not a part of the vpn subnet (10.0.200.0/24) The destination IP addresses is not the address of the end host (node n8 in private network)

(b) Can you see the data contents? Which device will decapsulate this IP datagram and decrypt this data?

No. Encrypted data by the vpn client. Will be decrypted by the vpn server.

(ii) Analyze the frame 1 captured in “FIT1047-2022-Applied-W9-Q3b.pcapng” and answer the following questions.

(a) What are the source and destination IP addresses used in the packets captured? Which device has inserted these IP datagrams in the private network?

IP-Source: 10.0.200.4, IP- Destination: 10.0.6.20

The source IP is a part of the vpn subnet (10.0.200.0/24) The destination IP addresses is the address of the end host (node n8 in private network)

(b) Can you see the data contents? Which device created this IP datagram contents?

Yes. IP datagram constructed by the vpn client, and later encrypted and encapsulated with the IP address of the host client PC and the vpn server PC. This packet is received by the vpn server to be decapsulated and decrypted later before sending it to the private network.