BISM3205 Assignment 1

**Daniel Ciccotosto-Camp**

S45857278

# Question 1 solns:

1. The first question deciphers to:

CONGRATULATIONSYOUHAVECOMPLETEDTHEFIRSTQUESTIONSUCESSFULLY

The Enigma machine uses a polyalphabetic substitution cipher, which is a type of cipher that replaces each letter in the plaintext with a different plaintext letter based on a series of substitution alphabets. The enigma machine introduces complexity into its polyalphabetic substitution using moveable rotors (I to VIII) which each internally had unique mappings of the English alphabet. When deciphering text, each keystroke caused the rightmost rotor to rotate one step so that subsequent text it would not be enciphered with the same ciphertext letter (piotte13, 2016).

Further complexity was added to the enigma machine with a plugboard, which allowed pairs of letters to be swapped before going through the moveable elements of the enigma. These components combined made the Enigma's encryption extremely complex and difficult to break without knowledge of the machine’s configuration settings.

1. The deciphered message from 1a), using the setting outlined in the task description, now becomes:

HJGCPHSIIELUKQTGGLXRCSHPCOQRQJEZDTINSGOOPRLIASQYSWXULGDISAH

# Question 2:



Phishing is a type of cyber-attack where attackers attempt to trick individuals into divulging personal or confidential information such as passwords or credit card details. This attack vector often involves deceptive emails, messages, or websites that appear legitimate but are crafted to manipulate the victim into sharing their sensitive data.

The term "phishing" was coined in the mid-1990s when cybercriminals used these tactics to impersonate AOL (America Online) staffers and message victims to reveal their passwords and credit card information.

1. What is spear phishing?

Spear phishing is a specialised and targeted phishing attack aimed at specific individuals within an organisation. Similar to phishing, cybercriminals craft personalised messages to deceive their victims into revealing sensitive information (including passwords or administrative access), which is especially valuable due to the extensive access and power the individual may provide within the company.

1. What is clone phishing?

Clone phishing is a phishing attack where an attacker replicates a legitimate email or message with a cloned message, replacing the contents with malicious links or malware under the guise as the original attachments. The cloned message is sent to the victim under the guise of it being a resend or update, to deceive them into engaging with harmful content.

1. What is whaling?

Whaling is a type of phishing attack that specifically targets high-profile individuals within an organisation, such as executives or senior managers. These type of phishing attacks use personalised messages to deceive high-target individuals into revealing sensitive information or authorising fraudulent transactions.

1. What is vishing?

Vishing, or ‘voice phishing’, is a type of phishing attack where attackers use phone calls or voice messages to deceive individuals into providing sensitive information, such as passwords, credit card numbers, or personal details. The attacker often impersonates a legitimate entity, such as a bank or government agency, to gain the victim's trust and trick them into revealing confidential information.

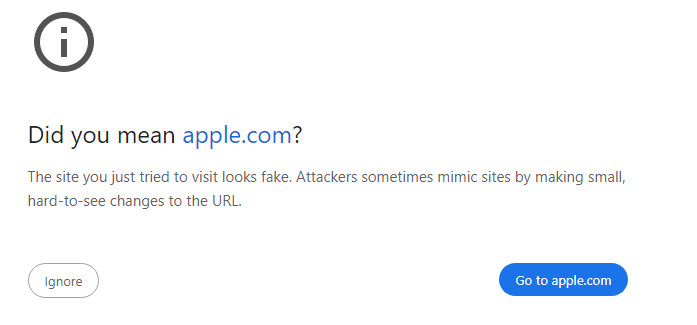
1. What is Pharming?

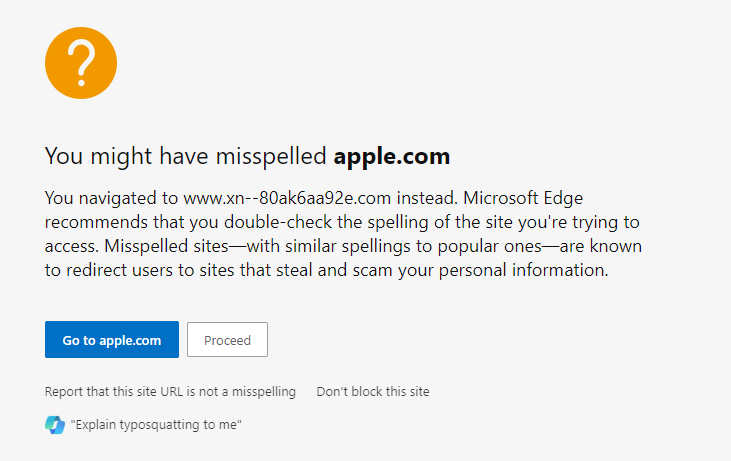
Pharming is a type of cyber attack where an attacker redirects a website's traffic to a fraudulent website without the user's knowledge. This is typically done by exploiting vulnerabilities in the DNS (Domain Name System) or compromising the user's device. The goal is to trick users into entering sensitive information, such as login credentials or financial details on the fake website, which looks almost identical to the legitimate one.

1. Homoglyph Attack

This type of attack is called a Homoglyph Attack. It works by using characters from different character sets that visually resemble standard characters but are actually different. In this case, the URL uses a character that looks almost identical to the standard letter ‘a’ but is actually a different Unicode character. When users click on the link, they may think they are visiting a legitimate site, such as "apple.com," but they are actually being directed to a malicious website that could be used for phishing or other types of cyber attacks. This kind of deception exploits the similarity between characters to trick users into visiting harmful websites.

The following browsers display warnings on a potential homoglyph attack.

Chrome:

Edge:

1. Preventative measures – Phishing attacks

Include security awareness in your organisation’s culture.

By raising awareness of the signs and dangers of phishing attacks, VPS employees will be able to identify them; be less likely to fall for them; or at least be able to flag an issue and report it to you so you can take timely steps to contain the incident.

Use spam filters or secure email gateways to block deceptive emails from reaching VPS employees.

Spam filters and secure email gateways monitor incoming emails for unwanted or fraudulent content. Once identified, they prevent them from ever reaching a VPS employee’s inbox.

Enable multifactor authentication (MFA) and anomaly login policies.

Even if an employee provides information to a scammer, these measures decrease a scammer’s ability to gain access to the employee’s work account and increase your ability to detect and respond to incidents in a timely manner.

Report phishing attempts to CIRS and OVIC.

You should report phishing attempts to the Victorian Government Cyber Incident Response Service by emailing cybersecurity@dpc.vic.gov.au who can help you respond to the incident.You should also report security incidents to OVIC by emailing a copy of our incident notification form to incidents@ovic.vic.gov.au or contacting us at privacy@ovic.vic.gov.au for privacy advice.

 **Employee Training and Awareness Programs**: Regularly train employees on how to recognize phishing attempts, including identifying suspicious emails, links, and attachments. This can include simulated phishing attacks to test and improve their response.

 **Implement Multi-Factor Authentication (MFA)**: Require multi-factor authentication for accessing sensitive systems and data. Even if an attacker obtains a user’s credentials, MFA adds an additional layer of security, making it harder for unauthorized access.

 **Email Filtering and Anti-Phishing Tools**: Use advanced email filtering and anti-phishing software that automatically detects and blocks phishing emails before they reach employees' inboxes. These tools can identify suspicious content and prevent it from being delivered.

 **Clear Reporting Mechanisms**: Establish clear and simple procedures for employees to report suspected phishing attempts. Quick reporting can help IT teams respond to threats more effectively and prevent widespread harm.



A 10Mbps (Megabits per second) digital communication device can send:

Assuming not latency, jitter and packet loss, all the bits sent could be ‘1’s in a digital signal, thus the most ‘1’ bits sent over a 10Mbps communication link is 10 million ().



The MD5 hash has known vulnerabilities, including its susceptibility to collision attacks (where two different inputs can produce the same hash value) and preimage attacks finding an input that hashes to a specific hash value). Because of known vulnerabilities, MD5 is no longer considered secure for protecting valuable data. In contrast, SHA-256, part of the SHA-2 family, addresses many of these issues by offering stronger security, better collision resistance, and a longer hash length.

**Mathematic comparison of brute-force time:**

MD5 generates a 129-bit has, leading to possible hashes.

Assuming an attacker can compute hashes per second:

However, due to MD5's known weaknesses, effective attacks could drastically reduce this time.

Compared to the SHA256 Hash, which generates a 256-bit hash:

Given these significant differences in security and the time required to brute-force, it would be better to use SHA-256 rather than MD5 to hash your valuable data before backing it up to prevent unauthorised access.

# Question 3

1. Identifying the Appropriate Notices

The TOLA Act provides three types of notices that law enforcement agencies can issue to communication providers: Technical Assistance Requests (TARs), Technical Assistance Notices (TANs), and Technical Capability Notices (TCNs).

**Technical Assistance Request (TAR):** This is a voluntary request where the AFP could ask SecureChat for assistance in accessing encrypted communications. However, it does not mandate compliance and is less likely to be effective if SecureChat is reluctant to cooperate.

**Technical Assistance Notice (TAN):** A TAN compels SecureChat to provide assistance that is within their existing capabilities, such as decrypting messages or providing metadata. This would be appropriate if the AFP believes SecureChat has the technical ability to assist without creating new tools or capabilities.

**Technical Capability Notice (TCN):** A TCN requires SecureChat to build new capabilities if they don't currently have the ability to assist. This is a stronger measure and would be used if SecureChat's existing capabilities are insufficient. However, TCNs are subject to stringent oversight due to their potential to create systemic weaknesses.

For the AFP’s case, issuing a **TAN** seems most appropriate. Since SecureChat is already an established encrypted messaging app, they likely have existing capabilities that the AFP could compel them to use. A TCN might be considered if SecureChat’s current capabilities are insufficient, but this would raise significant concerns about creating systemic vulnerabilities.

2. Legal and Procedural Requirements

The AFP must follow specific legal and procedural steps when issuing notices under the TOLA Act:

**Warrant and Legal Authority:** The AFP must have an existing legal authority, such as a warrant, before issuing a TAN or TCN. The warrant must be specific to the investigation and authorized by a judicial officer.

**Consultation Requirements:** Before issuing a TCN, the AFP must consult with SecureChat and the relevant communications provider industry body to discuss the potential impact and feasibility of the notice.

**Approvals and Oversight:** TANs and TCNs must be approved by a senior official, and TCNs require additional oversight by the Attorney-General and the independent statutory oversight bodies to ensure they do not create systemic weaknesses or vulnerabilities.

**Systemic Weaknesses:** The AFP must ensure that their requests do not force SecureChat to create systemic weaknesses or vulnerabilities in their encryption. The TOLA Act explicitly prohibits this, and the AFP must work closely with SecureChat to find a solution that meets the investigation's needs without compromising overall security.

3. Impact on Stakeholders

The issuance of notices under the TOLA Act can have significant impacts on SecureChat, its users, and society at large:`

**Impact on SecureChat:** Being compelled to assist law enforcement might strain SecureChat's resources and could damage its reputation if users perceive that their privacy is being compromised.

**Impact on Users:** Users may lose trust in SecureChat if they believe the platform can no longer guarantee the privacy of their communications. This could lead to a decline in user numbers and potential financial losses for SecureChat.

**Broader Societal Implications:** The balance between national security and privacy is a critical issue. While the TOLA Act aims to aid law enforcement, it raises concerns about overreach and the potential for abuse. If not managed carefully, the Act could undermine public trust in encrypted communications, leading to broader societal concerns about privacy and civil liberties.

# References

piotte13. (2016, Janurary 1). *Enigma Machine*. Retrieved from Enigma Mechanics: https://piotte13.github.io/enigma-cipher/