****

**DUBLIN INSTITUTE OF TECHNOLOGY**

**KEVIN STREET DUBLIN 8**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

#### BSc. (Honours) Degree in Computer Science

Year 3

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SUMMER EXAMINATIONS 2018**

\_\_\_\_\_\_\_\_\_\_\_\_

### Security [CMPU3034]

Dr. Y. Liu

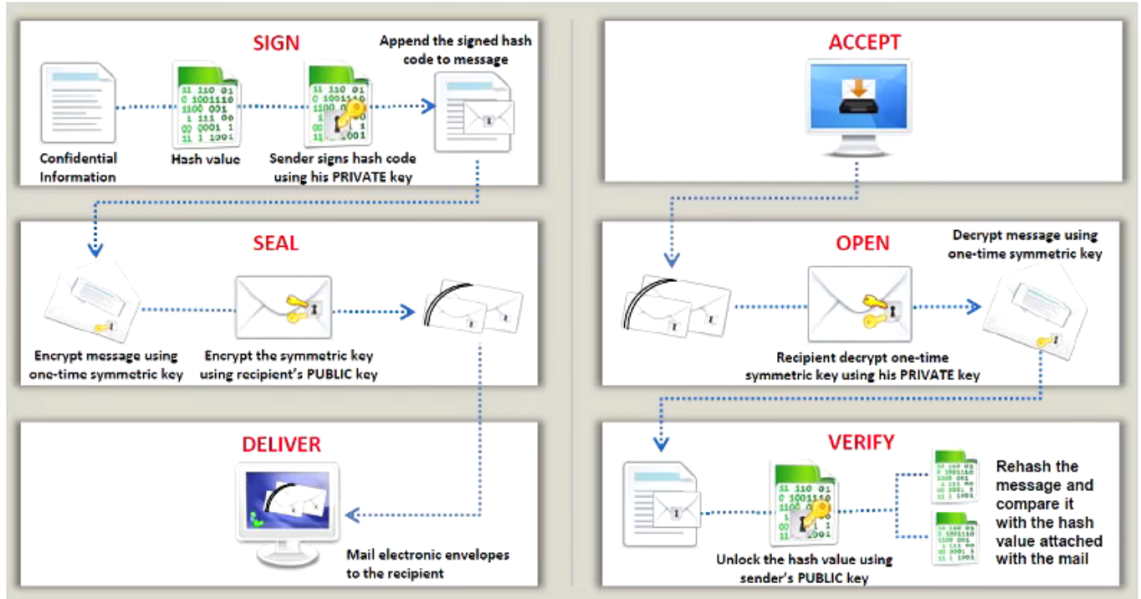
Dr. D. Lillis

Mr. P. Collins

Solution

# 1.

1. Secure Sockets Layer(SSL) is a protocol for D[ata encryption](https://en.wikipedia.org/wiki/Data_encryption)**and** decryption computer program that provides cryptographic privacy and authentication for data communication. Use a diagram to illustrate how Secure Sockets Layer(SSL) works? [10 marks]



1. Encrypt the following text by using the playfair Cipher ( pay no attention to space between the words ):

**FELLOW**

to encrypt this message (Key: ***CIPHER***) [10 marks]

FE

LX

LO

WX

**C I P H E  
R A B D F  
G K L M N  
O Q S T U  
V W X Y Z**

**NF**

**SP**

**GS**

**XY**

1. Alice wants to communicate with Bob, using RSA technology. The message that Alice wants to send Bob is the number 7. Alice selected two prime integers p=11, q=3. Use the RSA algorithm to help Alice generate private and public Keys. Also encrypt the message.

. [14 marks]

1. Check p = 7 and q = 13 are prime

2. n = pq = 91 and φ = (p − 1)(q − 1) = 72. [2 marks]

3. Choose e..

• Try e = 2. gcd(2,72) = 2 (does not work)

• Try e = 3. gcd(3,72) = 3 (does not work)

• Try e = 5. gcd(5,72) = 1 (it works) [3 marks]

e = 5.

4. Extend Eculident method

ex + φy = gcd(e, φ).

If e = 5 and φ = 72, we ﬁnd x = 29 and y = −2.

Indeed, 5(29) + 72(−2) = gcd(5,72) = 1. Then, [6 makrs]

d = 29.

5. The encryption function is E(M) = 10^5 mod 91=82 [3 marks ]

2.

1. **SQL injection (SQLi)** is an application security weakness that allows attackers to control an application’s database – letting them access or delete data, change an application’s data-driven behavior, and do other undesirable things – by tricking the application into sending unexpected SQL commands. List 6 ways to defending against SQLi Attacks. [12 marks]

1. **Employ comprehensive data sanitization**. Websites must filter *all* user input. Ideally, user data should be filtered for context. For example, email addresses should be filtered to allow only the characters allowed in an e-mail address, phone numbers should be filtered to allow only the characters allowed in a phone number, and so on.

2. **Use a web application firewall**. A popular example is the free, open source module [ModSecurity](http://www.modsecurity.org/) which is available for Apache, Microsoft IIS, and nginx web servers. ModSecurity provides a sophisticated and ever-evolving set of rules to filter potentially dangerous web requests. Its SQL injection defenses can catch most attempts to sneak SQL through web channels.

3. **Limit database privileges by context**. Create multiple database user accounts with the minimum levels of privilege for their usage environment. For example, the code behind a login page should query the database using an account limited only to the relevent credentials table. This way, a breach through this channel cannot be leveraged to compromise the entire database.

4. **Avoid constructing SQL queries with user input***.* Even data sanitization routines can be flawed. Ideally, using SQL variable binding with prepared statements or stored procedures is much safer than constructing full queries.

5. **Eliminate unnecessary database capabilities**, especially those that escalate database privileges and those that spawn command shells.

6. **Regularly apply software patches**. Because SQL injection vulnerabilities are regularly identified in commercial software, it is important to stay up to date on patching.

7. **Suppress error messages**. These messages are an important reconnaissance tool for attackers, so keep them local if possible. If external messages are necessary, keep them generic.

8. **Continuously monitor SQL statements from database-connected applications**. This will help identify rogue SQL statements and vulnerabilities. Monitoring tools that utilize machine learning and/or behavioral analysis can be especially useful.

1. Describe how Viruses can be categorised based on how they attack? Explain each type in detail.

[12 marks]

* Parasitic virus: traditional and still most common form of virus, it attaches itself to executable files and replicates when the infected program is executed (2 mark)
* • Memory-resident virus: Lodges in main memory as part of a resident system program, and infects every program that executes(2 mark)
* • Boot sector virus: Infects a master boot record and spreads when a system is booted from the disk containing the virus(2 mark)
* • Stealth virus: a virus explicitly designed to hide itself from detection by antivirus software(2 mark)
* • Polymorphic virus: mutates with every infection, making detection by the “signature”of the virus impossible. (2 mark)
* • Metamorphic virus: mutates with every infection, rewriting itself completely at each iteration changing behavior and/or appearance, increasing the difficulty of detection(2 mark)

1. Discuss the 5 steps to conduct successful penetration testing and ethical hacking projects. Use a diagram to help illustrate your answer.

[10 marks]

Must obtain a written agreement from the client.

Never exceed the limits of your authorization: Every assignment will have rules of engagement.

The tester should protect himself by setting up limitation as far as damage is concerned.

Be ethical: That's right; the big difference between a hacker and an ethical hacker is the word ethics.

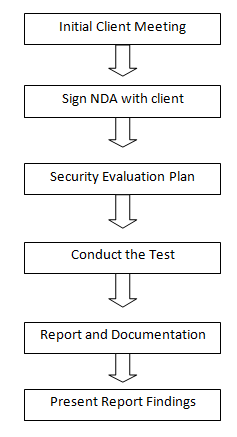
Maintain confidentiality: During security evaluations, you will likely be exposed to many types of confidential information.

Do no harm: It's of utmost importance that you do no harm to the systems you test.

Must have a detailed and tested plan before an assignment starts.

Scope of the engagement must be determined.

Understand business reasons (security breach or compliance) why the client wishes to perform ethical hacking. [5marks]

 f0102.eps

[5 marks]

3.

1. Steganography is the art and science of hiding information in a cover document such as digital images in a way that conceals the existence of hidden data. Discuss the disadvantages of using steganography.

[12marks]

Levels of Visibility: if the embedding process distorts the cover to the point that it is visually unnoticeable, meaning if the image is visibly distorted, then the carrier is insufficient for the payload. Likewise, if the image is not distorted, then the carrier is adequate.(3marks)

Robustness vs payload: Redundancy is needed for a robust method of embedding the message but it subsequently reduces the payload, robustness and payload are inversely related. Therefore, the smaller the pay load, the more robust it will be(3marks)

File format Dependence: Data compression techniques are of two types: lossy and lossless, Conversion of lossless information to compressed lossy information destroys the secret information present in the cover.

1. What are the advantages and disadvantages of **Symmetric** and **Asymmetric** Key Encryption Methods?

[8 marks]

Symmetric:

Advantage : any 3 points

Disadvantage: any 3 points

Asymmetric:

Advantage : any 3 points

Disadvantage: any 3 points

Advantages[2 marks]

- Simple: This type of encryption is easy to carry out. All users have to do is specify and share the secret key and then begin to encrypt and decrypt messages.

- Encrypt and decrypt your own files: If you use encryption for messages or files which you alone intend to access, there is no need to create different keys. Single-key encryption is best for this.

- Fast: Symmetric key encryption is much faster than asymmetric key encryption.

- Uses less computer resources: Single-key encryption does not require a lot of computer resources when compared to public key encryption.

- Prevents widespread message security compromise: A different secret key is used for communication with every different party. If a key is compromised, only the messages between a particular pair of sender and receiver are affected. Communications with other people are still secure.

Disadvantages [2 marks]

- Need for secure channel for secret key exchange: Sharing the secret key in the beginning is a problem in symmetric key encryption. It has to be exchanged in a way that ensures it remains secret.

- Too many keys: A new shared key has to be generated for communication with every different party. This creates a problem with managing and ensuring the security of all these keys.

- Origin and authenticity of message cannot be guaranteed: Since both sender and receiver use the same key, messages cannot be verified to have come from a particular user. This may be a problem if there is a dispute.

Asymmetric/Public Key Encryption

Advantages [2 marks]

- Convenience: It solves the problem of distributing the key for encryption.Everyone publishes their public keys and private keys are kept secret.

- Provides for message authentication: Public key encryption allows the use of digital signatures which enables the recipient of a message to verify that the message is truly from a particular sender.

- Detection of tampering: The use of digital signatures in public key encryption allows the receiver to detect if the message was altered in transit. A digitally signed message cannot be modified without invalidating the signature.

- Provide for non-repudiation: Digitally signing a message is akin to physically signing a document. It is an acknowledgement of the message and thus, the sender cannot deny it.

Disadvantages [2 marks]

- Public keys should/must be authenticated: No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

- Slow: Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.

- Uses up more computer resources: It requires a lot more computer supplies compared to single-key encryption.

- Widespread security compromise is possible: If an attacker determines a person's private key, his or her entire messages can be read.

- Loss of private key may be irreparable: The loss of a private key means that all received messages cannot be decrypted.

1. You have been tasked with introducing a new security policy in your company. The new policy allows employees to use laptops and other mobile devices at home, when travelling and on the company network. Discuss in detail how this policy can be safely rolled out without endangering the company network.

[12 marks]

First, you can use it to connect securely to a remote network via the Internet. Most companies maintain VPNs so that employees can access files, applications, printers, and other resources on the office network without compromising security, but you can also set up your own VPN to safely access your secure home network while you're on the road. (3 marks)

Second, VPNs are particularly useful for connecting multiple networks together securely. For this reason, most businesses big and small rely on a VPN to share servers and other networked resources among multiple offices or stores across the globe. Even if you don't have a chain of offices to worry about, you can use the same trick to connect multiple home networks or other networks for personal use. (3 marks)

Third, if you're concerned about your online privacy, connecting to an encrypted VPN while you're on a public or untrusted network—such as a Wi-Fi hotspot in a hotel or coffee shop—is a smart, simple security practice. Because the VPN encrypts your Internet traffic, it helps to stymie other people who may be trying to snoop on your browsing via Wi-Fi to capture your passwords. (3 marks)

Fourth and finally, one of the best reasons to use a VPN is to circumvent regional restrictions—known as geoblocking—on certain websites. Journalists and political dissidents use VPNs to get around state-sponsored censorship all the time, but you can also use a VPN for recreational purposes, such as connecting to a British VPN to watch the BBC iPlayer outside the UK. Because your Internet traffic routes through the VPN, it looks as if you're just another British visitor. (3 marks)