UNIVERSITI MALAYA
Centre for Continuing Education

# MASTER IN DATA SCIENCE

# FINAL EXAM

**COURSE CODE** : WQD7010

**COURSE TITLE** : NETWORK & SECURITY

**NAME** : NUR HIDAYAH BINTI AHMAD SHAFII

**MATRIC NUMBER** : 22120931

**CLASS** : 1

**LECTURER** : DR. SAAIDAL RAZALLI BIN AZZUHRI

1.a) The important design criteria for Stream Cipher are:

i. The encryption sequence should have a large period.
ii. The keystream should approximate the properties of a true random number stream as close as possible.
iii. The output of the pseudorandom number generator is conditioned on the value of the input key.

1.b.i)

$$k_i = k_{i-8} \oplus k_{i-6} \oplus k_{i-5} \oplus k_{i-1}$$
$$k = 11001110$$
$$k_9 = k_1 \oplus k_3 \oplus k_4 \oplus k_8 = 1 \oplus 0 \oplus 0 \oplus 0 = 1$$
$$k_{10} = k_2 \oplus k_4 \oplus k_5 \oplus k_9 = 1 \oplus 0 \oplus 1 \oplus 0 = 1$$
$$k_{11} = k_3 \oplus k_5 \oplus k_6 \oplus k_{10} = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$
$$k_{12} = k_4 \oplus k_6 \oplus k_7 \oplus k_{11} = 0 \oplus 1 \oplus 1 \oplus 1 = 1$$
$$k_{13} = k_5 \oplus k_7 \oplus k_8 \oplus k_{12} = 1 \oplus 1 \oplus 0 \oplus 1 = 1$$
$$k_{14} = k_6 \oplus k_8 \oplus k_9 \oplus k_{13} = 1 \oplus 0 \oplus 1 \oplus 1 = 1$$
$$k_{15} = k_7 \oplus k_9 \oplus k_{10} \oplus k_{14} = 1 \oplus 1 \oplus 1 \oplus 1 = 0$$
$$k_{16} = k_8 \oplus k_{10} \oplus k_{11} \oplus k_{15} = 0 \oplus 1 \oplus 1 \oplus 0 = 0$$

$$k' = k_9 k_{10} k_{11} k_{12} k_{13} k_{14} k_{15} k_{16} = 11111100$$

1.b.ii)

m XOR k' = 11010110 XOR 11111100 = 00101010
Therefore, the resulting ciphertext produced with the stream cipher is 00101010

1.c.i)

$$c_o = random\ IV$$
$$c_i = E(k, m_i \oplus c_{i-1})\ for\ i = 1, .., n$$

1.c.ii)

$$c_o = random\ IV$$
$$c_i = E(k, c_o + i) \oplus m_i\ for\ i = 1, .., n$$

1.d.i) The S-boxes in DES are nonlinear substitution boxes. It introduces non-linearity and confusion into the encryption process. Confusion is the characteristic of ensuring that the relationship between the plaintext and the ciphertext is complex. Non-linearity is the characteristic of assuring that even minor modifications to the input lead to substantial changes in the output. The DES utilizes 8 S-boxes each with a 6 bit input and 4 bit output. Consequently, the 48 bit input will be converted to a 32 bit output after the S-boxes are employed. S-boxes introduce confusion to the data and key by mapping inputs to random outputs through substitution. It transforms the intermediate values generated during encryption into different values based on predefined substitution tables. The DES is therefore challenging to decrypt using linear or differential cryptanalysis.

1.d.ii)

$$S_1X_1 = S_1(000000) = 1111$$
$$S_1X_2 = S_1(000001) = 0011$$
$$S_1X_1 \oplus S_1X_2 = 1111 \oplus 0011 = 1100$$
$$S_1(X_1 \oplus X_2) = S_1(000000 \oplus 000001) = S_1(000001) = 0011$$
$$Since\ 1100 \neq 0011.\ Hence, S_1X_1 \oplus S_1X_2 \neq S_1(X_1 \oplus X_2)$$

1.d.iii) It shows that for given inputs $X_1 = 000000$ and $X_2 = 000001$ , the output of DES S-box $S_1$ does not satisfy the property $S_1X_1 \oplus S_1X_2 \neq S_1(X_1 \oplus X_2)$. This lack of linearity and predictability is important because it shows that the S-box introduces the necessary non-linearity and complexity into the encryption process. Hence, it increases the cryptographic strength of DES by making it resistant to linear and differential cryptanalysis.

2.a) Let $e = 5, p = 7\ and\ q = 17$

$$(p-1)(q-1) = (7-1)(17-1) = 96$$

Check gcd(96,5):

$$96 = 5\,.19 + 1$$
$$5 = 1\,.5 + 0$$

Therefore, gcd(96,5)=1.
Hence, the condition $\gcd\big((p-1)(q-1), e\big) = 1$ is satisfied

$$n = pq = 7(17) = 119$$
$$n = pq = 7(17) = 119$$

$$\phi(\mathrm{n}) = (p-1)(q-1) = (7-1)(17-1) = 96$$

$$D = \frac{(p-1)(q-1)(e+1)+1}{e} = \frac{96(6)+1}{5} = 115.4$$

D should be an integer but 115.4 is not an integer, While $e = 5, p = 7\ and\ q = 17$ satisfy the condition similar to RSA but the formula provided does not produce an integer value of D. Therefore, the scheme as described with these parameters does not align with the standard RSA algorithm.

2.b.i) Let M1=(2,3), M2=(1,4) and n=5

For M1, h(M1)=(2+3)mod 5=5mod 5= 0

For M2, h(M2)=(1+4)mod 5=5mod 5= 0

Since both values has the same hash value 0, it indicates a collision. Therefore, it does not satisfy the requirement of uniformity and avalanche effect. It may not evenly distribute hash values across the output space, and small changes in the input may not lead to significant changes in the hash value.

2.b.ii) ) Let M1=(2,3), M2=(1,4) and n=5

For M1, h(M1)=13 mod 5 =3

For M2, h(M2)=17 mod 5 =2

Since the values for both M1 and M2 is different, it shows that it has better uniformity and avalanche properties

2.b.iii) $= (237^2 + 913^2) = 889738$
h(M) = $889738\ mod\ 757$ = 263

2. c.i) 43 72 79 70 74 6F

2.c. ii) t0 = IV = 2A 01 (given)
For the first block (m1 = 43 72):

- t1 = E(k, m1 $\oplus$ t0)
- m1 $\oplus$ t0 = 43 72 $\oplus$ 2A 01 = 69 73
- Find E(k, 69 73) from the given encryption samples:

    - E(k, 69 73) = 1A E7
- So, t1 = 1A E7

For the second block (m2 = 79 70):

- t2 = E(k, m2 ⊕ t1)
- m2 ⊕ t1 = 79 70 ⊕ 1A E7 = 63 17
- Find E(k, 63 17) from the given encryption samples:
    - E(k, 63 17) = 30 5A
- So, t2 = 30 5A

For the third block (m3 = 74 6F):

- t3 = E(k, m3 ⊕ t2)
- m3 ⊕ t2 = 74 6F ⊕ 30 5A = 44 35
- Find E(k, 44 35) from the given encryption samples:
    - E(k, 44 35) = E2 B5
- So, t3 = E2 B5

Calculate the final tag t**:**

- t = E(k, t3)
- t3 = E2 B5 (from the previous step)
- Find E(k, E2 B5) from the given encryption samples:
    - E(k, E2 B5) = 9C A2
- So, t = 9C A2

Therefore, the tag (MAC) of the message "Crypto" using the CBC-MAC with the provided block cipher operations and encryption samples is 9C A2**.**

3. a) The ingredients of an authentication server's ticket are:

i. C = Client requesting access
ii. AS = Authentication Server
iii. V = server whose services or application that is required
iv. IDc= Identifier of user on C
v. IDv – Identifier of V
vi. Pc = password of user on C
vii. ADc = network address of client
viii. Kv = secret encryption key shared by AS and V
ix. TS = timestamp indicating when the ticket was issued or when it expires.
x. Lifetime = the duration for which the ticket is valid
xi. Kc,v = session key shared between the client and the server
xii. || = concatenation

These ingredients are combined into a structured format that allows the authentication server to verify the authenticity of the ticket and grant access accordingly.

3. b) AS will receive a message from C and will check the database for user ID and password match and the permission whether the user has access to V (server). If passed, it will take the user as authentic and AS will generate a ticket. The ticket will contain user ID, server ID and network address, all encrypted by a secret key shared by AS and V. V will receive a message from C with C's ID and the ticket. V decrypts the ticket and will verify whether the user ID in the ticket is the same as in the unencrypted ID. Matches result will lead the server to grant the requested service. The ticket is encrypted to prevent forgery. ADc is included to counter reply to attacks.

3. c) Network access control (NAC) refers to the management of network access. NAC authenticates users who connect into the network and determines the data they can access and the actions they can take. Additionally, NAC also examines the health of the user's computer or mobile device (the endpoints)

3. d) A cloud computing reference architecture is a framework or blueprint that offers a structured approach to the design, implementation, and management of cloud computing solutions. It identifies the vital components and their interactions that are required to establish a cloud environment that is both scalable and resilient. Enterprises, developers, and cloud providers utilize the architecture as a framework to develop cloud services and applications that satisfy business needs. The cloud consumer, cloud provider, cloud carrier, cloud auditor and cloud broker are the five primary performers of cloud computing reference architecture. In cloud computing, each performer is an object (a person or an organization) that takes part in a transaction or process and/or executes tasks.

i. Cloud Providers: Cloud Provider A person, organization, or entity responsible for making a service available to interested parties.
ii. Cloud Auditor: A party that can conduct independent assessment of cloud services, information system operations, performance and security of the cloud implementation.
iii. Cloud Broker: An entity that manages the use, performance and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.
iv. Cloud Carrier: An intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.

In addition, Platform as a Service (PaaS), Software as a Service (SaaS), and Infrastructure as a Service (IaaS) are other important components of cloud computing service providers.

i. IaaS Providers: The infrastructure components would be present in an on-premises data center. These elements encompass the virtualization layer, networking, storage, and servers.
ii. SaaS Providers: The infrastructure components allow each user to access programs via the internet, instead of having to install the software on the user's computer
iii. PaaS Providers: a third-party provider delivers hardware and software tools to users over the internet. Usually, these tools are needed for application development. A PaaS provider hosts the hardware and software on its infrastructure.

There are four deployment models for cloud computing reference architectures namely public cloud, private cloud, hybrid cloud, and community cloud.

i. Public cloud: The cloud infrastructure and resources are given to the public via a public network. These models are generally owned by companies that sell cloud services.
ii. Private cloud: The cloud infrastructure and resources are only accessible by the cloud consumer. These models are generally owned by cloud consumers themselves or a third party.
iii. Hybrid cloud: It consists of a mixture of different deployment models like public, private, or community. This helps in the exchange of data or applications between various models.
iv. Community cloud: The cloud consumers might share their cloud infrastructure and resources as they may have the same goal and policies to be achieved. These models are owned by organizations or third-party.

4. a) The smallest building block of a wireless LAN is a basic service set (BSS), which consists of wireless stations executing the same MAC protocol and competing for access to the same shared wireless medium. A BSS may be isolated, or it may connect to a backbone distribution system (DS) through an access point (AP). The building block of an 802.11 WLAN is a set of basic services consisting of wireless stations running the same MAC protocol and competing for access to the same shared wireless medium. The BSS is the basic building block of an 802.11 WLAN. Each BSS area roughly corresponds to the coverage of some stations. A central concept of a BSS is that all stations must 'hear' each other, that is, be within radio or optical range. The association between stations is dynamic, stations can come in and out of range or be switched off. To become a member of a BSS, each station must become associated to the network. These associations are dynamic and are managed and maintained using a distribution system service (DSS). 802.11 WLAN architectures are integrated with others using portals.

4. b) The partnership consists of agreeing on a set of capabilities to be used for security. It allows a mobile node that has made a transition to identify itself to the access point (AP) within a basic service set (BSS) so that the node can participate in data exchanges with other mobile nodes.

4. c) A blended attack refers to a highly advanced cyber-attack that mixes multiple methods and strategies in order to accomplish its goals. These attacks commonly combine many methods of attack, such as exploiting software vulnerabilities, social engineering, phishing, malware propagation, and other methods in order to increase their effectiveness and avoid being detected. There are several characteristics of blended attacks include:

i. Multiple Attack Vectors: Blended attacks exploit various vulnerabilities and methodologies either at the same time or in a certain order. For example, an attacker might use a phishing email to deliver malware that exploits a software vulnerability upon execution.

ii. Complexity: It is frequently complex and well-planned attack that need knowledge of several areas such as programming, social engineering, and network infiltration.

iii. Goal Diversity: Blended attacks can have diverse goals, including data theft, financial fraud, network disruption, or simply causing chaos.

iv. Adaptability: It can be difficult to mitigate and defend against attackers since they can modify their strategies in real time in response to defenses detected.

v. Stealth and Persistence: By using multiple attack vectors, blended attacks can be stealthy and persistent, allowing attackers to maintain access or continue exploitation over an extended period.

Advanced persistent threats (APTs) are a type of blended attack in which the attacker uses social engineering techniques, malware that has been specially created, and phishing emails to penetrate a network and stay hidden for a long time. Strong network security, user education and awareness programs, software patching, intrusion detection systems, and incident response plans help organizations defend against blended attacks.

4. d) The difference between a reflector DDoS attack and a direct DDoS attack are

i) Reflector DDoS attack

- In a reflector DDoS attack, the attacker makes use of a potentially legitimate third-party component to send the attack traffic to a victim, ultimately hiding the attacker's own identity.

- The attacker then sends spoofed requests to these reflector servers, making it appear that the requests originated from the target (victim) IP address.
- It is difficult to trace the source of the attack back to the originating devices.
- Reflector DDoS attacks are more complex to execute since attackers need to identify and exploit intermediary servers (reflectors) that will respond to spoofed requests.
- It can significantly amplify the attack traffic.

ii) Direct DDoS attack

- In a direct DDoS attack, the attacker directly sends a high volume of malicious traffic to flood a targeted resource.
- The traffic generated in a direct DDoS attack originates directly from the devices controlled by the attacker.
- It is easier to trace the source of the attack back to the originating devices.
- Direct DDoS attacks are generally simpler to execute since attackers directly send a large volume of traffic to the target without relying on intermediary servers.
- It lacks of amplification.