THE PAPUA NEW GUINEA UNIVERSITY OF TECHNOLOGY

DEPARTMENT OF ELECTRICAL AND COMMUNICATIONS ENGINEERING

FINAL EXAMINATION (2021)
SEMESTER 2

EE496 – Network Security Management

FORTH YEAR (ELECTRICAL) BEEL 4

TIME ALLOWED: 3 HOURS

INFORMATION FOR STUDENTS

1. You have **TEN (10) MINUTES** to read the paper.
   You must not begin writing during this time.

2. **Answer all questions.**

3. All answers must be written in the **ANSWER BOOK** supplied.

4. **COMPLETE THE DETAILS REQUIRED ON THE FRONT COVER OF YOUR ANSWER BOOK – DO THIS NOW.**

5. Textbooks and laptops **ARE NOT** permitted.

6. If you are found cheating in the Examination, the penalties specified by the University shall apply.

7. TURN OFF all Mobile Phone and place them on the floor under your seat before the start of Examination

Question 1 True of False [10 Marks]

Questions [1 marks each]	Answer: True | False
A) SHA2 is a hashing an algorithm use for secure hashing	
B) Symmetric Key Algorithms are prone to key replay attack when operating under ECB mode	
C) AES and MD5 are BOTH Symmetric Key Algorithms for generating cipher text	
D) NIST is a Certificate Authority	
E) The algorithm of AES is published publicly	
F) The algorithm of SHA-512 is never published publicly	
G) AES is used in generating digital signatures	
H) Diffie-Hellman can be used in generating digital signatures	
I) The complexity of solving the discrete logarithm problem in modulus arithmetic is the reason why public key cryptography works.	
K) Public key cryptography and asymmetric key cryptography are both difference names of the same thing.	

Question 2: Multiple Choices [10 Marks]

Which of the following entities dictates how the crypto algorithm transforms back and forth between the original data and the obfuscated one **[2 marks]**:			
A) plain text	B) cipher text	C) key	D) nonce

An example of a public key cryptographic algorithm is **[2 marks]**:			
A) MD5	B) ECDH	C) Triple DEC	D) SHA2

To increase the security of a crypto-algorithm which of the following must be done **[2 marks]**?			
A) Use a larger key	B) Don't publish the algorithm publicly	C) publish the algorithm publicly	D) none of the given options

The purpose of digital signatures is to **[2 marks]**:			
A) bind the digital data to the digital certificate	B) Obfuscate the digital data to keep is secret	C) Authenticate the digital data related to an entity	D) none of the given options

An example of a secure hash function is **[2 marks]**:			
A) AES	B) ECDH	C) Triple DEC	D) SHA2

Question 3 Symmetric key Encryption [10 marks]

RC4 is an example of a stream cipher for which it generate encrypted data through XORing a stream of pseudorandom bits. The algorithm is used in many popular networking technologies such as secured Wifi and SSL. However, As of 2015, there is speculation that some state cryptologic agencies may possess the capability to break RC4 when used in secured protocol.

1. [3 marks] Explain why it is difficult to recover the original data when it is encrypted by XORing against a stream of random bits using the concept of: XOR operation, plain text, and repeating patterns.
2. [3 marks] Unlike a modern stream cipher, RC4 does not take a separate nonce alongside the key. Explain why in the absence of a nonce shall weaken the algorithm using the concept of: XOR operation, plain text, and repeating patterns.
3. [2 marks] Explain why secure WIFI uses RC4 instead of Triple-DES as the means to provide secure data transmission using the concept of pipe-lining and ciphering-rounds even-though it is DES3 that is more secure.
4. [2 marks] Explain why Triple-DES is still being used (instead of newer algorithms) in some newer digital products thought the concept of monetary cost and data security.

Question 4 Public key cryptography [10 Marks]

RSA is a public-key cryptosystem that is widely used for secure data transmission. The following questions relates to a scenario where Alice and Bob are trying the establish a secure channel for message exchange and Darth is trying to uncover the sent messages issued by the two parties without authorization.

A) [4 marks] Assuming that Alice wish to securely send a message to Bob and both parties have agreed on what symmetric key cryptosystem to use. Explain the steps via actions conducted by Alice and Bob of how the use of RSA helps establish a common key for both Alice and Both without Darth discovering it.

B) [4 marks] Assuming Bob whats to authenticate that the other party, whom he communicates with, is the real Alice. Using the concept of PKI Explain the steps via actions conducted by Alice, Bob, and the CA of how the use of RSA helps accomplish this task.

C) [2 marks] Give two reasons why it is symmetric-key and not public-key cryptosystems is used as the general means to encrypt messages.

Question 5 Secure Network Communication [10 Marks]

Name and describe the steps used by TLS 1.2 for establishing a secure channel of communication.