College of Computer Studies
Sultan Kudarat State University
Isulan, Sultan Kudarat

IAS322 – Information Assurance and Security 2
MIDTERM

Name: _____ Section: _____

Test I: True or False (2 points each item a total of 30 points)
Write T if the statement is True and F if the statement False.

_____1. Cybersecurity is only the responsibility of IT professionals, not employees.

_____2. Regularly updating software and applications helps protect against security vulnerabilities.

_____3. Ransomware encrypts files and demands payment for their release.

_____4. Cybercriminals only target financial institutions and big companies

_____5. Antivirus software can protect against all types of cyber threats

_____6. Using the same password for multiple accounts is a good security practice.

_____7. Phishing attacks trick users into providing personal information by pretending to be a trustworthy source.

_____8. Encryption retrieve the original data

_____9. Decryption converts plaintext to protect data

_____10. Symmetric encryptions use different key

_____11. Asymmetric encryption uses two key public and private keys

_____12. The purpose of encryption is to make data unreadable forever.

_____13. Cryptography is only useful for securing online transactions

_____14. Algorithm a sequence of step how to solve problem

_____15. The Caesar cipher uses a different key for encryption and decryption

Testing II: Matching Type (2 points each item a total of 20 points)
*Match the type in **Column A** with its definition in **Column B**. Write your answer in the provided space.*

_____1. Pretexting
_____2. Baiting
_____3. Algorithm
_____4. Caesar Algorithm
_____5. Phising
_____6. Security Consultant

_____7. Ethical Hacker
_____8. Security Architect
_____9. Chief Information Security Officer
_____10. Cryptography

Column A (Terms)		Colum B (Descriptions)	
1	Pretexting	a	Is the Science of encoding and decoding information to prevent unauthorized access.
2	Baiting	b	Oversee day to day operations.
3	Algorithms	c	Cybersecurity professional who serves as an adviser and consultant about technology. Assess Security Risk and Threats.
4	Caesar Algorithm	d	Cybersecurity professional who's in charge of maintaining company security and staying updated on the latest security trends and threats.
5	Phishing	e	Is a social engineering attack that lures victims with something tempting, like free coupon, promo or downloads, to spread malware or steal data.
6	Security Consultant	f	Step-by-step procedure or set of rules designed to solve a problem or perform a task.
7	Ethical Hacker	g	form of social engineering attack where a cybercriminal creates a false identity or scenario to trick a victim into revealing sensitive information**.**
8	Security Architect	h	Is a social engineering attack where attackers use fake emails or websites to trick victims into revealing sensitive information like passwords or credit card details.
9	Chief Information Security Officer	i	Cybersecurity professional who lawfully tests and secures systems by finding and fixing vulnerabilities before malicious hackers can exploit them.
10	Cryptography	j	Is one of the simplest and most well-known encryption techniques.

Test III: Problem Solving (50 pts)
Show your solution, and put your answer on the back of this questionnaire.

Encrypt the plaintext message:
"Hello, World!" using ChaCha20 Algorithm. Find the ciphertext (hexadecimal output).
Using the following parameters:
a. 256-bit Key (32 bytes, in hexadecimal)
b. 96-bit Nonce (12 bytes, in hexadecimal)
c. Counter: 1 (starting from 1 instead of 0)

Prepared by:

KRISTINE MAE H. AMPAS, MIT
Faculty

Reviewed by:

CERILO B. RUBIN, JR, MIT
Faculty Program Chairperson, BSIT

Approved:

ELBREN O. ANTONIO, DIT
Dean, College of Computer Studies