Name: _____ **Date:** _____

Student Number: _____ **Section:** _____ **Score:** _____

ITP115 – Cryptography
Midterm Examination
2nd semester, A.Y. 2024-2025

I. MATCHING TYPE

Direction: Write the correct answer from the box.

A. Cryptanalysis	**F.** Nonrepudiation	**K.** Monoalphabetic substitution cipher	**P.** Dictionary attack	**U.** Diffie-Hellman Key Exchange
B. Cryptography	**G.** Private Key	**L.** Polyalphabetic substitution cipher	**Q.** Frequency analysis	**V.** Digital signature
C. Confidentiality	**H.** Public Key	**M.** Substitution cipher	**R.** Kasiski examination	**W.** Hash function
D. Information security	**I.** Secret Key	**N.** Transposition cipher	**S.** Advanced Encryption Standard	**X.** Mode of operation
E. Integrity	**J.** Block cipher	**O.** Brute force attack	**T.** Data Encryption Standard	**Y.** RSA algorithm

_____ 1. It is the study of using algorithms to protect information.
_____ 2. It is the process of identifying weaknesses to decrypt a message without a key.
_____ 3. It ensures that only authorized people can access data.
_____ 4. It ensures that all information is complete and accurate.
_____ 5. It ensures that a user cannot deny making a transaction.
_____ 6. It is used in symmetric-key ciphers for both encryption and decryption.
_____ 7. It is used in asymmetric-key ciphers for encryption and is shared openly.
_____ 8. It is used in asymmetric-key ciphers for decryption and is kept secret.
_____ 9. It replaces each letter in the plaintext with another letter.
_____ 10. It rearranges the letters of the plaintext.
_____ 11. It is a type of substitution cipher that uses multiple alphabets to encrypt the plaintext.
_____ 12. It encrypts a group of plaintext symbols.
_____ 13. It finds how often symbols appear in encrypted text and compares them to the English alphabet to reveal the message.
_____ 14. It is the process of determining the length of a Vigenère cipher key.
_____ 15. It is an attempt to find the key by testing it against a set of words.
_____ 16. It was the first encryption standard used for unclassified U.S. government applications.
_____ 17. Also known as the Rijndael algorithm, it is the encryption standard used today.
_____ 18. It is a technique for enhancing the effect of a cryptographic algorithm.
_____ 19. It helps two parties create a shared secret over an insecure channel.
_____ 20. It is an asymmetric algorithm based on the difficulty of factoring large prime products.

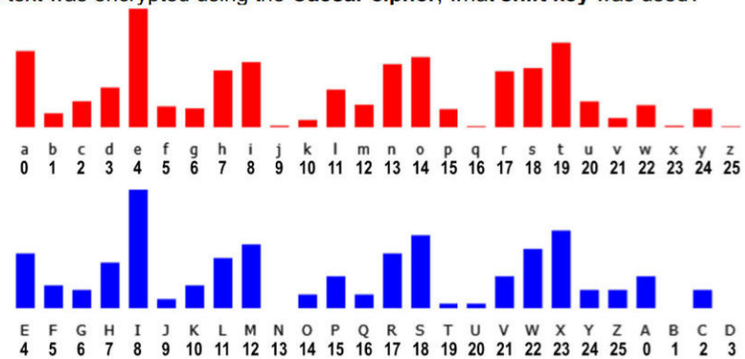
II. MULTIPLE CHOICE

Direction: Shade the circle of the correct answer.

1. The **first diagram** shows **letter frequencies** in **standard English text**, while the **second** shows **letter frequencies** in your **ciphertext**.

   If the text was encrypted using the **Caesar cipher**, what **shift key** was used?

   ○ A ○ B ○ C ○ D



   A. E
   B. I
   C. S
   D. X

2. If you encrypt the word **"SYMMETRICKEY"** using the **Playfair cipher**, what **digraphs** will you use?

   ○ A ○ B ○ C ○ D

   A. SY-MM-ET-RI-CK-EY
   B. SY-MM-ET-RI-CK-EY-X
   C. SY-MX-ME-TR-IC-KE-Y
   D. SY-MX-ME-TR-IC-KE-YX

3. If you use the word **"CRYPTOGRAPHY"** as the **Playfair cipher key**, what will your **key square** look like?

   ○ A ○ B ○ C ○ D

   A.

C	R	Y	P	T
O	G	R	A	P
H	Y	C	R	Y
P	T	O	G	R
A	P	H	Y	C

   C.

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

B.

C	R	Y	P	T
O	G	R	A	P
H	Y	A	B	C
D	E	F	G	H
I/J	K	L	M	N

D.

C	R	Y	P	T
O	G	A	B	C
D	E	F	G	H
I/J	K	L	M	N
O	P	Q	R	S

Answer items 4 and 5 to find the Vigenère cipher key length using Kasiski examination.

4. **"OCI"** is a **repeating sequence** in the ciphertext. What is the **distance** between them? ○ ○ ○ ○ A B C D

KWWWQCDVGMGPITRYKPKTFIEJCSPOJCBVCNXMKWNEFJSGIOCAB
CNDSEBENRCSCIQYRCZVGFEROOCIELNSLOTSLPGMOCIHYDERRE
RSWCXGPITROHUSXFKTSLPGMELNTPSZYDIIOCPOUSSVCCFMDLR
RINEFJSGIOCYXHRRIPOGGZMCXXQZVGFEROOCIXMLIBOGPITRO

A. 12 **C.** 14
B. 13 **D.** 15

5. The table shows repeating sequences, their distances, and factors. ○ ○ ○ ○ A B C D

What is the possible Vigenère cipher **key length**?

Repeating Sequence	Distance	Factor
TSLP	33	3, 11, 33
ZVGF	108	2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 108
NEFJ	111	3, 37, 111
GPIT	180	2, 3, 4, 5, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180

A. 2 **C.** 4
B. 3 **D.** 6

6. Which **rail fence pattern** was used to encrypt the ciphertext **"MLAUAAGMNNO"**? ○ ○ ○ ○ A B C D

A.

M				O				L		
	A		N		N		U		A	
		A				G				M

C.

M								L		
	A						U		A	
		A				G				M
			N		N					
				O						

B.

M						G				
	A				N		U			
		A		O				L		M
			N						A	

D.

M										M
	A								A	
		A						L		
			N				U			
				O		G				
					N					

7. The Social Security System (SSS) website uses the cipher suite **TLS_AES_256_GCM_SHA384** for secure communication. ○ ○ ○ ○ A B C D

What is the **key size** of the AES encryption used in this cipher suite?

A. 128 **C.** 256
B. 192 **D.** 384

8. Alice and Bob use Diffie-Hellman key exchange with prime **p = 7** and generator **g = 3**. Alice chooses a private key **a = 2**, and Bob shares his public key **B = 6**. What is their **shared secret key** using the formula B^a **mod p**? ○ ○ ○ ○ A B C D

A. 0 **C.** 5
B. 1 **D.** 6

9. A shared secret **should not be used directly** as an **encryption key**. Instead, you can use a **hash function** like **SHA** to generate a key. The output size depends on the SHA variant. For example, **SHA-224 gives 224 bits.** ○ ○ ○ ○ A B C D

If we use **AES-256** for encryption, which **SHA variant** should we use?

A. SHA-224 **C.** SHA-384
B. SHA-256 **D.** SHA-512

10. The security of RSA is based on the difficulty of integer factorization. Which pair of prime numbers **multiplies** to **221**? ○ ○ ○ ○ A B C D

A. 7 and 11 **C.** 19 and 23
B. 13 and 17 **D.** 29 and 31

III. TRUE OR FALSE
Direction: Write **T** if the statement is **true** and **F** if it is **false**.

_____ 1. If the **key** is a **15-letter English word**, **brute force** is **more efficient** than a **dictionary attack**.
_____ 2. **Hill Climbing** can find a **Playfair cipher key** that is **different** from the **original** but **still correctly decrypts** the ciphertext.
_____ 3. **Data Encryption Standard (DES)** and **Advanced Encryption Standard (AES)** are examples of **asymmetric-key** ciphers.

_____ 4. **DES** uses **only one round of encryption**.
_____ 5. **DES** is **still secure** and **remains uncrackable** with modern computing power.
_____ 6. The **National Privacy Commission** advises government agencies to use **AES-256** encryption **to protect personal information**.
_____ 7. **RSA** is **slower than AES** because it uses **more complex mathematical operations.**
_____ 8. **AES** uses **elliptic curves** for **encryption**.

IV. ENCRYPTION

Direction: **Complete the questions.**
Use the table below to convert the symbols into numbers.

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

1. **(3 pts)** Encrypt the word **"CRYPTO"** using the **Caesar cipher**, with the **first letter of your first name** as the **shift key.**
   - What is the **first letter** of your **first name**?

     ✓ _____
   - What is its corresponding **numerical value**?

     ✓ _____
   - Convert the **letters to numbers**.

Plaintext	C	R	Y	P	T	O
p	61	82	89	80	84	79

   - Add the **shift key k** to **p**. This means calculating **p + k**.

Plaintext	C	R	Y	P	T	O
p + k	____	____	____	____	____	____

   - Apply **modulo 26**. This means calculating **(p + k) mod 26**.

Plaintext	C	R	Y	P	T	O
(p + k) mod 26	____	____	____	____	____	____

   - What is the **ciphertext** in **symbols**?

     ✓ _____

2. **(3 pts)** Encrypt the word **"CRYPTO"** using the **Vigenère cipher**, with the **first three letters of your first name** as the **key**.
   - What is the **first three letters** of your **first name**?

     ✓ _____ _____ _____
   - What are their corresponding **numerical values**?

     ✓ _____ _____ _____
   - Convert the **letters to numbers**.

Plaintext	C	R	Y	P	T	O
p	61	82	89	80	84	79

   - Match **each letter** of the **plaintext** with a **letter** from the **key**.

Plaintext	C	R	Y	P	T	O
p	61	82	89	80	84	79
k (Letter)	____	____	____	____	____	____

   - Convert **each letter** of the key **into a number**.

Plaintext	C	R	Y	P	T	O
p	61	82	89	80	84	79
k (Number)	____	____	____	____	____	____

   - Add the **shift key k** to **p**. This means calculating **p + k**.

Plaintext	C	R	Y	P	T	O
p + k	____	____	____	____	____	____

   - Apply **modulo 26**. This means calculating **(p + k) mod 26**.

Plaintext	C	R	Y	P	T	O
(p + k) mod 26	____	____	____	____	____	____

   - What is the **ciphertext** in **symbols**?

     ✓ _____

3. **(3 pts)** Encrypt the word **"CRYPTO"** using the **Playfair cipher**.
   - What are the **last two digits** of your **student number**?
     Example: *The* ***last two digits*** *of* ***25B1234*** *are* ***34****.*

     ✓ _____
   - Apply **modulo 5** to the **number**:

     ✓ _____
   - Based on **your result**, choose the **Playfair cipher key** to use.

Result	Key
0	ANALYSIS
1	CURRENCY
2	GRAPHY
3	MINING
4	SYSTEM

   - What is your **key**?

     ✓ _____
   - Use **your key** to create a **5x5 key square**.

   - What **digraphs** can you form from the plaintext **"CRYPTO"**?

     ✓ _____ _____ _____
   - Use **your key square** to **encrypt** the **digraphs**.

     ✓ _____ _____ _____

4. **(3 pts)** Encrypt the plaintext **"CYBERSECURITY"** using the **Rail Fence cipher**.
   - What is the **last digit** of your **student number**?
     Example: *The* ***last digit*** *of* ***25B1234*** *is* ***4****.*

     ✓ _____
   - Take the **number** and use it to **create a rail fence with that many rows.**
     Then, **place each letter** from the plaintext in the **correct position**.
     Ignore the spaces and commas in the plaintext.

     <u>If your number is 0, 1, or 2, use 3 as the number of rows instead.</u>

   - What is the **ciphertext**?

     ✓ _____