

NHÓM 1

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = SAVEFORARAINYDAY

Key: K = 25

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = WHENINROMEDO

Key: K = THETRU

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = BARKINGDOGSS

Key: K = LIKEFA

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = PENNYWISEPOUNDFO

Key: K = KGOXPMUHCAYTJQWZRIVESFLDNB

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = STILLWATERSR

Key: K = SAVEFORA

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = TIMEISMONEYTIMEISM

Key: K = 5

Tìm Output: C =

NHÓM 2

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. MẬT MÃ CAESAR

Input: M = AWOMANGIVESANDFO
Key: K = 11
Tìm Output: C = LHZXLYRTGPDLYOQZ

2. MẬT MÃ VIGENERE – LẮP KHÓA

Input: M = HONESTYISTHEBE
Key: K = ABADBE
Tìm Output: C = 7 15 13 7 19 23 24 9 18 22 8 8 1 5
-> H P N H T X Y J S W I I B F

3. MẬT MÃ VIGENERE – AUTOKEY

Input: M = HONESTYISTHEBE
Key: K = ABADBEHONESTYI
Tìm Output: C = 7 15 13 7 19 23 5 22 5 23 25 23 25 12
---> H P N H T X F W F X Z X Z M

4. MÃ HÓA CHỮ ĐƠN

Input: M = LIKEFATHERLIKESO
Key: K = LYFGMKNERXJPQIVATOHSDZBUCW
Tìm Output: C = PRJMKLSEMOPRJMHV

5. MẬT MÃ MA TRẬN KHÓA PLAYFAIR

Input: M = SOFARSOGOODSO
Key: K = EASTORW
Tìm Output: C =

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

chèn X: SO FA RS OG OX OD SO
==> TE GE BE AK SZ DK TE

6. MẬT MÃ HOÁN VỊ

Input: M = WHENINROMEDOASTHER
Key: K = 4
Tìm Output: C =

W	R	A
H	N	O
E	I	M
N	E	H

-> WRAHNOOSREIMDTENEH

NHÓM 3

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = NOROSEWITHOUTATH

Key: K = 8

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = MONEYMAKESTHE

Key: K = YOUREON

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = MONEYMAKESTHE

Key: K = YOUREON

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = AWOMANGIVESANDFO

Key: K = THLEYNPSXADWKFUBOGMQVJRCIZ

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = THETRUTHWILLOU

Key: K = THEDIEIS

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = ABADBEGINNINGMAKES

Key: K = 9

Tìm Output: C =

NHÓM 4

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = STILLWATERSRUNDE

Key: K = 17

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = THETRUTHWILLO

Key: K = THEGRASS

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = THETRUTHWILLO

Key: K = THEGRASS

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = MONEYMAKESTHEMAR

Key: K = JEHFAVZNOXUBMYPKDLGSRCTWQI

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = ACLEANFASTISB

Key: K = EASTO

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = HONESTYISTHEBESTPO

Key: K = 6

Tìm Output: C =

NHÓM 5

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = YOUREONLYYOUNGON

Key: K = 8

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = ABADBEGINNIN

Key: K = MENMAKE

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = ABADBEGINNIN

Key: K = MENMAKE

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = WHENINROMEDOASTH

Key: K = HLXQPSVKMZYCDUEGJTNFBIAIWOR

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = WHENINROMEDO

Key: K = MONEYIS

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = THEDIEISCASTTHEDIE

Key: K = 8

Tìm Output: C =

NHÓM 6

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = STILLWATERSRUNDE

Key: K = 25

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = PRACTICEMAKESP

Key: K = TWOCANP

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = PRACTICEMAKESP

Key: K = TWOCANP

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = TIMEISMONEYTIMEI

Key: K = KGOXPMUHCAYTJQWZRIVESFLDNB

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = ALLWORKANDNOP

Key: K = BEAUTYIS

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = THEGRASSAREALWAYSG

Key: K = 7

Tìm Output: C =

NHÓM 7

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = ITSASMALLWORLDIT

Key: K = 22

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = BETTERSAFETH

Key: K = ITSASM

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = BETTERSAFETH

Key: K = ITSASM

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = ONESWALLOWDOESNT

Key: K = WBXGIHOVSYMFUAKZJNCPQLTRED

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = ITSANILLBIRD

Key: K = NOROSEW

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = DONTTROUBLETROUBLE

Key: K = 7

Tìm Output: C =

NHÓM 8

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = LOVEISBLINDLOVEI

Key: K = 8

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = MONEYMAKESTH

Key: K = NOPAIN

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = MONEYMAKESTH

Key: K = NOPAIN

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = THEGRASSAREALWAY

Key: K = HLXQPSVKMZCYCDUEGJTNFBIAIWOR

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = LOVEISBLINDL

Key: K = HONESTY

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = DONTTROUBLETROUBLE

Key: K = 8

Tìm Output: C =

NHÓM 9

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = ABADBEGINNINGMAK

Key: K = 18

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = LOVEISBLINDLOVE

Key: K = WHENIN

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = LOVEISBLINDLOVE

Key: K = WHENIN

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = EVERYONEHASTHEIR

Key: K = PEINVRXLASWCBYHMOFGKZUQDTJ

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = BEAUTYISONLYSK

Key: K = BEAUTY

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = NOPAINNOGAINNOPAIN

Key: K = 9

Tìm Output: C =

NHÓM 10

YÊU CẦU CHUNG

1. Hiểu được khái niệm **Mã hóa cổ điển và Mật mã hiện đại**
2. Hiểu được khái niệm **An toàn tuyệt đối và An toàn tính toán**
3. Hiểu được khái niệm **tấn công vét cạn (Brute-force) và Phân tích mã (Cryptanalysis)**
4. Hiểu được khái niệm **Mô hình mã hóa đối xứng và Mô hình mã hóa không đối xứng**

BÀI TẬP

1. **MẬT MÃ CAESAR**

Input: M = LOVEISBLINDLOVEI

Key: K = 21

Tìm Output: C =

2. **MẬT MÃ VIGENERE – LẶP KHÓA**

Input: M = MONEYISAGOODSER

Key: K = EVERYONE

Tìm Output: C =

3. **MẬT MÃ VIGENERE – AUTOKEY**

Input: M = MONEYISAGOODSER

Key: K = EVERYONE

Tìm Output: C =

4. **MÃ HÓA CHỮ ĐƠN**

Input: M = WHENINROMEDOASTH

Key: K = HLXQPSVKMZCYDUEGJTNFBIAIWOR

Tìm Output: C =

5. **MẬT MÃ MA TRẬN KHÓA PLAYFAIR**

Input: M = BEAUTYISINTHEE

Key: K = ITSASMA

Tìm Output: C =

6. **MẬT MÃ HOÁN VỊ**

Input: M = WHENINROMEDOASTHER

Key: K = 5

Tìm Output: C =