Nhóm 6

Đề tài 39 Trình bày các phương pháp mã hóa cổ điển, xây dựng chương trình mô phỏng thuật toán Affine

Học phần: An toàn bảo mật thông tin
Lớp: DCCNTT 13.10.16

Các Thành Viên

Họ và Tên	Mã Sinh Viên
Nguyễn Trí Dũng	20223155
Nguyễn Trung Chính	20222999
Vũ Văn Phong	20222998
Trần Văn Nam	20222996
Đổng Trung Đức	20222877

Đại Học Công Nghệ Đông Á

Nội Dung

1. GIỚI THIỆU CÁC MÃ HÓA CỔ ĐIỂN
2. NGUYÊN LÝ HOẠT ĐỘNG MÃ HÓA AFFINE
3. DEMO CHƯƠNG TRÌNH AFFINE

1

GIỚI THIỆU CÁC MÃ HÓA CỔ ĐIỂN

Vigenère Cipher

01

a, Bảng chữ cái Vigenère

Bảng Vigenère là một ma trận kích thước 26x26, trong đó mỗi hàng là một dịch chuyển của bảng chữ cái chuẩn (A-Z). Bảng này được sử dụng để mã hóa văn bản bằng cách thay thế mỗi ký tự của văn bản bằng một ký tự khác dựa trên từ khóa.

b, Quy trình mã hóa

Văn bản gốc và từ khóa được sắp xếp sao cho mỗi ký tự của từ khóa ứng với một ký tự của văn bản gốc. Nếu từ khóa ngắn hơn văn bản, nó sẽ được lặp lại liên tục. Mỗi ký tự trong văn bản gốc được thay thế bằng một ký tự từ bảng Vigenère, tương ứng với vị trí của ký tự đó trong từ khóa...

Vigenère Cipher

c, Ưu điểm của Vigenère Cipher:

- Khó phá mã hơn so với Caesar Cipher: Do sử dụng một từ khóa để thay đổi cách dịch chuyển ký tự, Vigenère Cipher không lặp lại các mẫu dịch chuyển giống nhau, giúp tăng độ phức tạp trong việc phá mã bằng phương pháp tần số ký tự thông thường.

- Bảo mật tốt hơn cho các văn bản dài: Nhờ việc sử dụng từ khóa có độ dài khác nhau, Vigenère Cipher giúp tránh lặp lại các mẫu dịch chuyển cố định, làm cho việc nhận diện các mẫu khó hơn so với các mật mã dịch chuyển đơn giản.

Vigenère Cipher

d, Nhược điểm của Vigenère Cipher:

- Dễ bị phá nếu từ khóa ngắn hoặc lặp lại: Khi từ khóa ngắn hoặc được sử dụng lặp lại nhiều lần, kẻ tấn công có thể sử dụng phương pháp Kasiski hoặc phân tích tần số để phát hiện ra từ khóa và giải mã văn bản.

- Không bảo mật trước các cuộc tấn công bằng phân tích tần số hiện đại: Mặc dù Vigenère Cipher vượt trội hơn Caesar Cipher, nhưng với các phương pháp phân tích hiện đại, nó vẫn có thể bị phá mã khi kẻ tấn công có đủ văn bản mã hóa.

Vigenère Cipher

Cách thức thực hiện:

Để mã hóa, ta dùng một hình vuông Vigenère. Nó gồm 26 hàng, mỗi hàng dịch về bên trái một bước so với hàng phía trên, tạo thành 26 bảng mã Caesar. Trong quá trình mã hóa, tùy theo từ khóa mà mỗi thời điểm ta dùng một dòng khác nhau để mã hóa văn bản.

Ví dụ, ta có văn bản cần mã hóa như sau: ATTACKATDAWN

Người gửi lựa chọn một từ khóa và viết nó lặp lại nhiều lần trên một dòng đến khi số chữ cái trên dòng bằng số chữ cái trong thông điệp, với từ khóa "LEMON" thì:

Vigenère Cipher

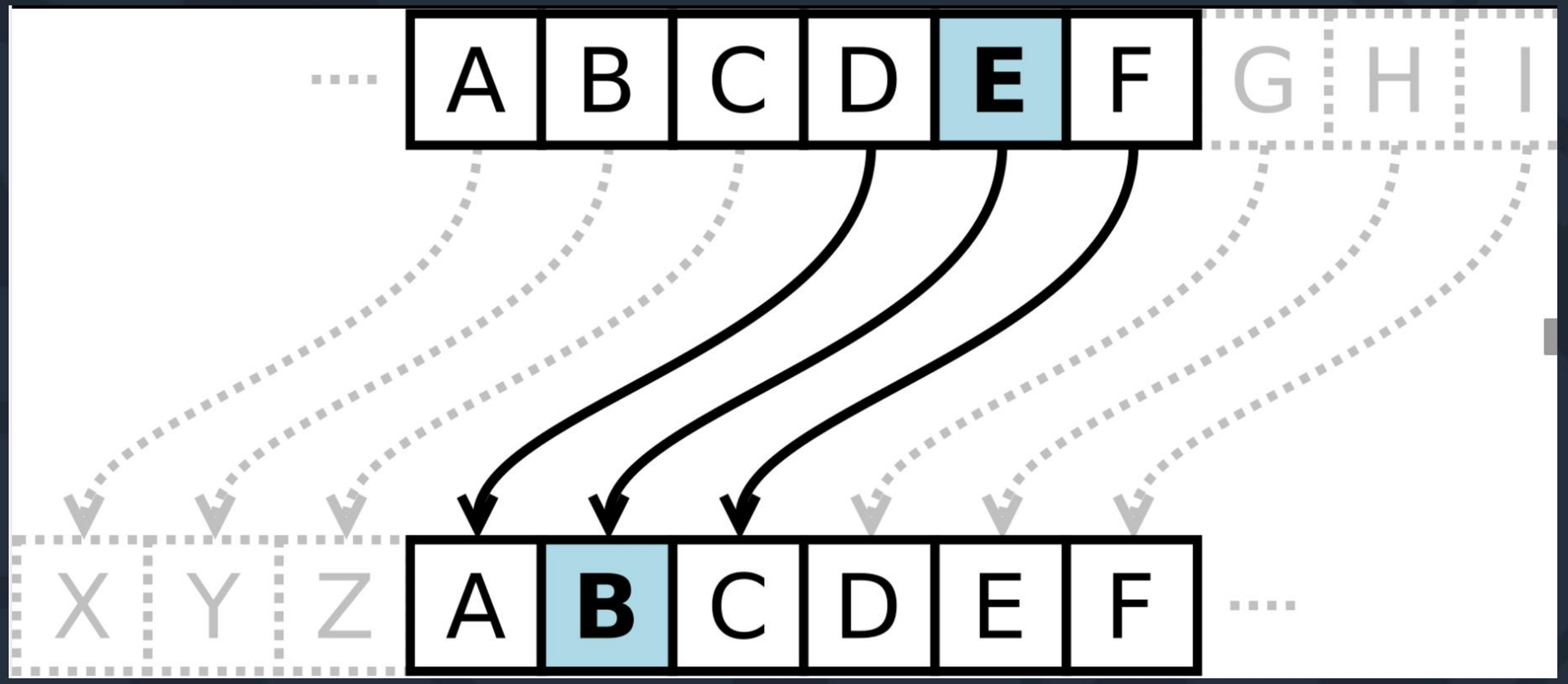
Văn bản:	ATTACKATDAWN
Từ khóa:	LEMONLEMONLE
Bản mã:	LXFOPVEFRNHR

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

Chữ cái đầu tiên của văn bản, A, được mã hóa bằng bảng bắt đầu với L (chữ cái đầu tiên của từ khóa). Nó sẽ được mã hóa thành chữ cái trên dòng L và cột A của hình vuông Vigenère, đó là chữ L. Tương tự như vậy, chữ cái thứ hai của văn bản sẽ được mã hóa bằng chữ cái thứ hai của từ khóa: chữ trên dòng E và cột T là X.

Caesar Cipher

Khái niệm về Caesar Cipher, còn được gọi là Caesar Shift, là một phương pháp mã hóa cổ điển, trong đó mỗi ký tự trong văn bản gốc được thay thế bằng một ký tự khác trong bảng chữ cái theo một khoảng cách cố định.



Caesar Cipher

a, Ưu điểm của Caesar Cipher:

- Đơn giản và dễ hiểu: Phương pháp mã hóa này rất dễ thực hiện và dễ dàng hiểu. Chỉ cần dịch chuyển các ký tự trong bảng chữ cái theo một số nguyên nhất định.

- Nhanh chóng: Việc mã hóa và giải mã bằng Caesar Cipher diễn ra nhanh chóng, đặc biệt với các văn bản ngắn, vì chỉ cần thực hiện phép toán số học đơn giản.

b, Nhược điểm của Caesar Cipher:

- Bảo mật kém: Caesar Cipher dễ bị tấn công bằng các phương pháp như phân tích tần số, vì số lượng khóa rất hạn chế (chỉ có 25 khóa khác nhau cho bảng chữ cái tiếng Anh).

- Không phù hợp cho dữ liệu nhạy cảm: Vì bảo mật thấp, phương pháp này không thích hợp cho việc bảo vệ thông tin quan trọng hoặc nhạy cảm, khi mà an ninh là yếu tố cần thiết.

Caesar Cipher

Quy trình mã hóa: Đối với bảng mã tiếng anh (ABCDEFGHI...), nếu độ dịch là 3, A sẽ được thay bằng D, B sẽ được thay bằng E, ..., W sẽ thay bằng Z, X sẽ thay bằng A, Y sẽ thay bằng B và Z thay bằng C.

Để mã hóa, người ta đánh số các chữ cái từ 0 -> N-1 (N là tổng số phần tử của bản chữ cái). Không gian khóa K=ZN. Với mỗi khóa K K hàm mã hóa và giải mã một ký tự có số thứ tự là I sẽ được biểu diễn như sau: EK(i) = (i+k) mod 26

Caesar Cipher

Văn bản:	TOIYEUVIETNAM
Khóa:	4
Bản mã:	YSMBYZWMIYREQ

Bản rõ	T	O	I	Y	E	U	V	I	E	T	N	A	M
i	19	14	8	23	4	20	21	8	4	19	13	0	12
(i+k) mod N	23	18	12	1	8	24	25	12	8	23	17	4	16
Bản mã	Y	S	M	B	Y	Z	W	M	I	Y	R	E	Q

Playfair Cipher

a, Bảng chữ cái

Playfair Cipher sử dụng một bảng chữ cái 5x5 để mã hóa. Trong bảng này, các chữ cái từ A đến Z được sắp xếp, với I và J được coi là cùng một ký tự để phù hợp với bảng 5x5. Nó là một trong những phương pháp mã hóa đa ký tự sớm nhất, thay vì mã hóa từng ký tự riêng lẻ như Caesar Cipher.

b, Cấu trúc

Bảng chữ cái 5x5 được tạo ra bằng cách chọn một từ khóa. Các chữ cái trong từ khóa sẽ được điền vào bảng trước, sau đó các chữ cái còn lại sẽ được điền vào cho đến khi bảng hoàn thành.

Playfair Cipher

c, Ưu điểm của Playfair Cipher:

- Bảo mật tốt hơn Caesar Cipher: Playfair sử dụng các cặp ký tự thay vì từng ký tự đơn, làm cho phân tích tần số trở nên khó khăn hơn. Điều này giúp tăng cường tính bảo mật so với các phương pháp đơn giản hơn.

- Khó đoán hơn: Sử dụng ma trận 5x5 cho các ký tự, Playfair tạo ra nhiều khả năng mã hóa khác nhau, khiến cho việc dự đoán và tấn công trở nên phức tạp hơn.

Playfair Cipher

d, Nhược điểm của Playfair Cipher:

- Phức tạp hơn trong thực hiện: So với các phương pháp như Caesar Cipher, Playfair yêu cầu nhiều bước hơn trong cả quá trình mã hóa và giải mã, có thể gây khó khăn cho người mới.

- Vẫn dễ bị tấn công: Mặc dù bảo mật tốt hơn, Playfair Cipher vẫn có thể bị tấn công bằng các phương pháp phân tích tần số hoặc các kỹ thuật tấn công khác, nhất là khi có nhiều văn bản được mã hóa.

2

NGUYÊN LÝ HOẠT ĐỘNG MÃ HÓA AFFINE

Affine Cipher

a, Khái niệm cơ bản

Affine Cipher là một phương pháp mã hóa thay thế dựa trên sự kết hợp giữa phép nhân và phép cộng theo mô-đun. Mã hóa Affine sử dụng hai tham số (thường gọi là khóa) để mã hóa mỗi ký tự trong văn bản gốc.

b, Cấu trúc

Phương trình mã hóa trong Affine Cipher là:

$$E(x)=(a*x+b)\bmod 26$$

Trong đó:

E(x) là ký tự được mã hóa.

a và b là các khóa mã hóa (với điều kiện UCLN(a,26)=1).

x là vị trí của ký tự trong bảng chữ cái (ví dụ: A=0, B=1,... Z=25).

Affine Cipher

c, Quy trình mã hóa

Chọn khóa: Người mã hóa chọn hai số nguyên aaa và bbb, với điều kiện aaa và 26 phải nguyên tố cùng nhau (tức là UCLN(a,26)=1UCLN(a, 26) = 1UCLN(a,26)=1).

Chuyển đổi ký tự thành số: Mỗi ký tự trong văn bản gốc được ánh xạ vào một số từ 0 đến 25.

Áp dụng công thức mã hóa: Áp dụng công thức $E(x)=(a \times x+b) \bmod 26$ để mã hóa từng ký tự.

Chuyển đổi số trở lại ký tự: Các số sau khi mã hóa được chuyển đổi lại thành ký tự trong bảng chữ cái.

Quy trình giải mã ngược lại với công thức: $D(x)=a-1 \times (x-b) \bmod 26$

Affine Cipher

d, Ưu điểm

- Đơn giản và dễ triển khai: Phương pháp mã hóa Affine có cấu trúc đơn giản, dễ hiểu và dễ thực hiện trong các ứng dụng mã hóa cổ điển.
- Mã hóa đa biến: Sự kết hợp giữa phép nhân và phép cộng giúp Affine Cipher mạnh mẽ hơn so với các phương pháp mã hóa chỉ dựa trên phép dịch chuyển, như Caesar Cipher.

Affine Cipher

e, Nhược điểm

- Dễ bị tấn công phân tích tần số: Do chỉ có 26 ký tự, Affine Cipher vẫn dễ bị phá mã thông qua các kỹ thuật phân tích tần số. Kẻ tấn công có thể phân tích sự xuất hiện thường xuyên của các ký tự để xác định khóa.
- Số lượng khóa hạn chế: Chỉ có một số giá trị nhất định của aaa và bbb có thể sử dụng, vì aaa phải nguyên tố cùng 26, nên số lượng khóa có thể sử dụng bị giới hạn.

Affine Cipher cung cấp một mức bảo mật cơ bản, nhưng không được khuyến nghị sử dụng trong các ứng dụng mã hóa hiện đại.

Affine Cipher

- Hệ mã Affine là một loại mã hóa đối xứng thuộc nhóm mã hóa theo phép dịch tuyến tính. Trong hệ mã này, mỗi ký tự trong bản rõ (plaintext) sẽ được biến đổi thành ký tự mã hóa (ciphertext) bằng một công thức tuyến tính phụ thuộc vào hai tham số: khóa a và b.
- Khóa (a, b) trong mã hóa affine là một cặp số dùng để chuyển đổi một ký tự trong bảng chữ cái thành một ký tự khác theo công thức:

$$E(x)=(a*x+b) \bmod 26$$

Trong đó : E(x) là ký tự được mã hóa.

x là chỉ số của ký tự gốc.

a và *b* là các tham số của khóa.

Affine Cipher

Mã hóa affine hoạt động theo hai bước chính:

1. Chuyển đổi chỉ số ký tự: Đầu tiên, mỗi ký tự trong bảng chữ cái được chuyển đổi thành chỉ số của nó (ví dụ: A = 0, B = 1, ..., Z = 25).

2. Áp dụng công thức mã hóa: Sử dụng công thức:

$E(x) = (a * x + b) \bmod m$

Tính toán giá trị mới cho chỉ số ký tự bằng cách nhân chỉ số gốc x với a, sau đó cộng b, và lấy phần dư theo m (số ký tự trong bảng chữ cái).

3.Chuyển đổi lại thành ký tự: Cuối cùng, chỉ số mới được chuyển đổi trở lại thành ký tự tương ứng.

Affine Cipher

Cho $\mathcal{P} = \mathcal{C} = Z_{26}$ và giả sử

$$\mathcal{P} = \{ (a,b) \in Z_{26} \times Z_{26} : \text{UCLN}(a,26) = 1 \}$$

Với $K = (a,b) \in \mathcal{K}$, ta định nghĩa:

$$e_K(x) = ax + b \bmod 26$$

và

$$d_K(y) = a^{-1}(y-b) \bmod 26,$$

$x,y \in Z_{26}$

Affine Cipher

Giả sử K = (3,6). Hàm mã hóa là: eK(x) = 3x + 6. Ta mã hóa bản rõ “xung”. Trước tiên biến đổi các chữ x, u, n, g thành các thặng dư theo modulo 26. Ta được các số tương ứng là: 23, 20, 13, 6. Bây giờ ta sẽ mã hóa :

3*23 + 6 mod 26 = 75 mod 26 = 23.

3*20 + 6 mod 26 = 66 mod 26 = 14.

3*13 + 6 mod 26 = 45 mod 26 = 19.

3*6 + 6 mod 26 = 24 mod 26 = 24.

Vậy 4 kí hiệu của bản mã là 23, 14, 19, 24 tương ứng xâu kí tự là : “xoty”

Affine Cipher

Và hàm giải mã tương ứng là: dK(y) = 9(y-6) = 9y – 2. Vậy 4 kí hiệu của bản mã là 23, 14, 19, 24 tương ứng xâu kí tự là : “xoty”.

Bên cạnh đó chúng ta sẽ có cách giải mã những ký tự vừa mã hóa ở trên. Đó là:

Việc giải mã sẽ áp dụng thuật toán giải mã dK đã tính toán ở trên :

9*23 – 2 mod 26 = 205 mod 26 = 23.

9*14 – 2 mod 26 = 124 mod 26 = 20.

9*19 – 2 mod 26 = 169 mod 26 = 13.

9*24 – 2 mod 26 = 214 mod 26 = 6.

Bản rõ sau khi giải mã là “xung”.

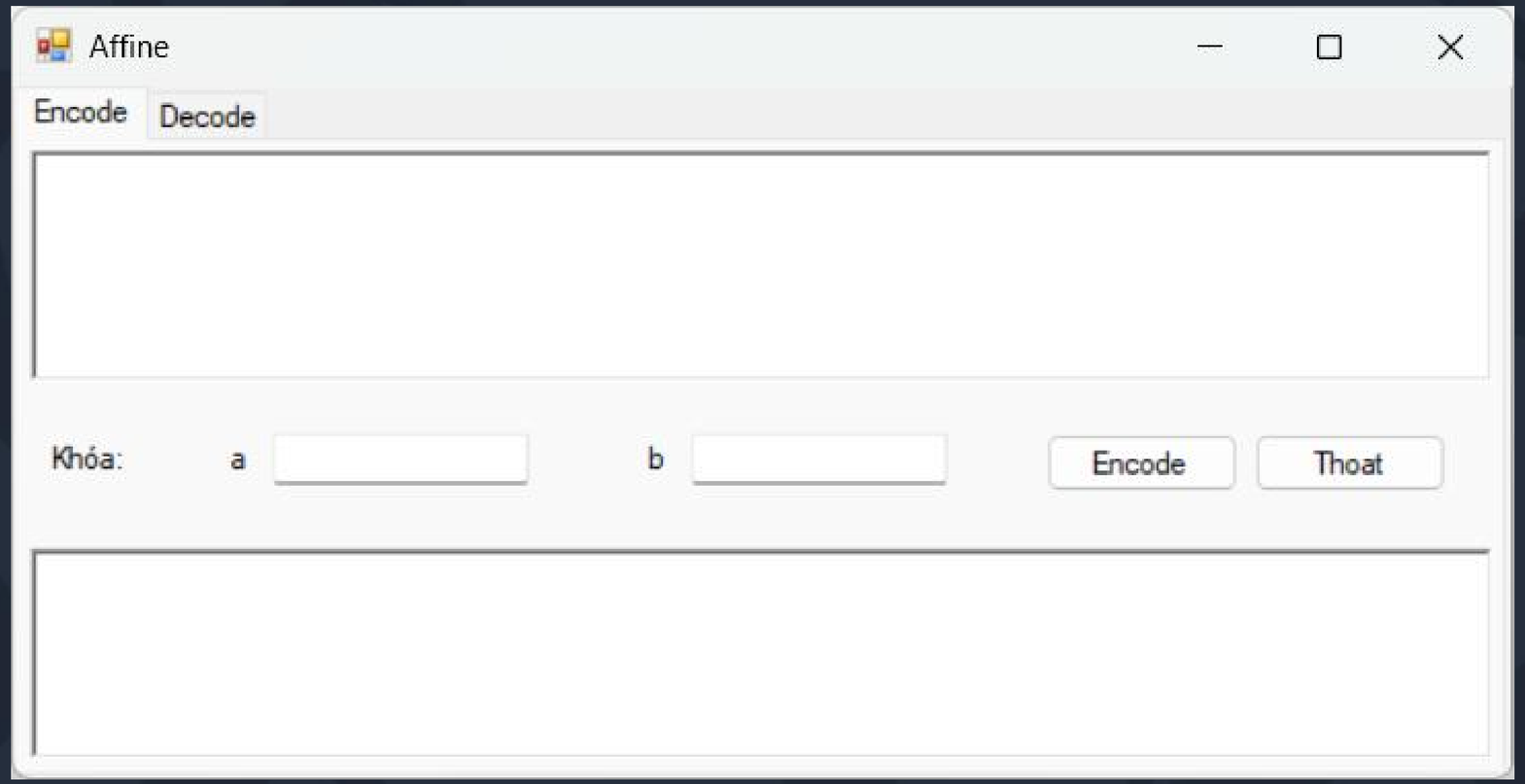
3

DEMO CHƯƠNG TRÌNH AFFINE

Demo mã affine

Kết quả thu được

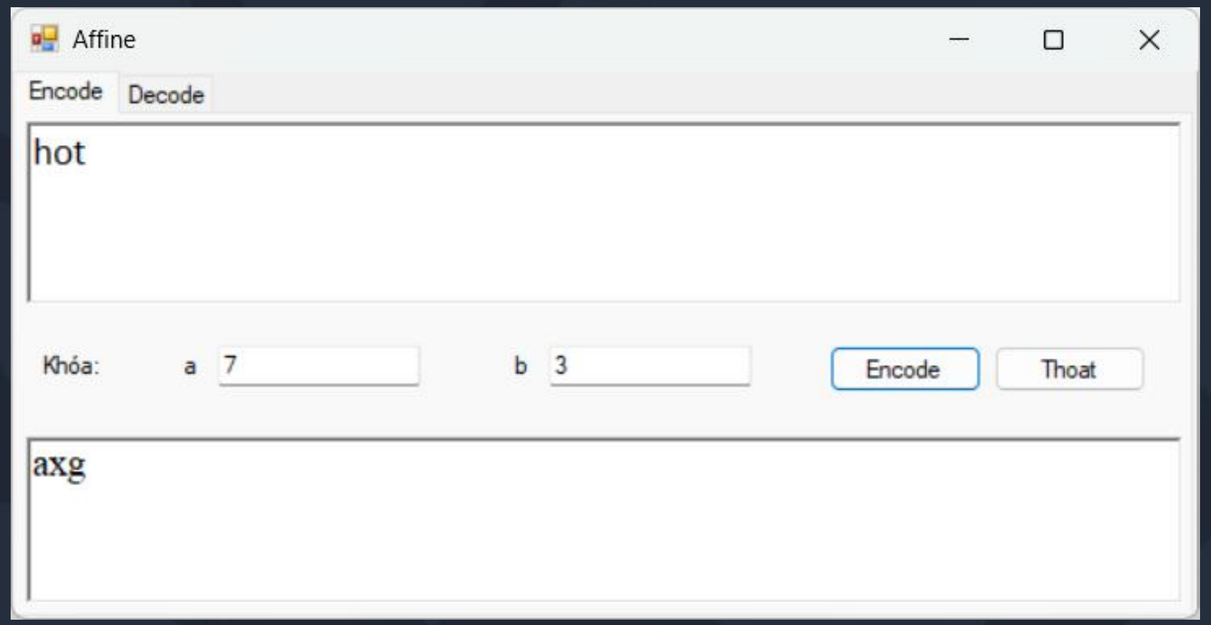
Chương trình hoạt động tốt sau khi hoàn thành và khởi chạy. Dưới đây là thành quả thu được của chúng tôi:



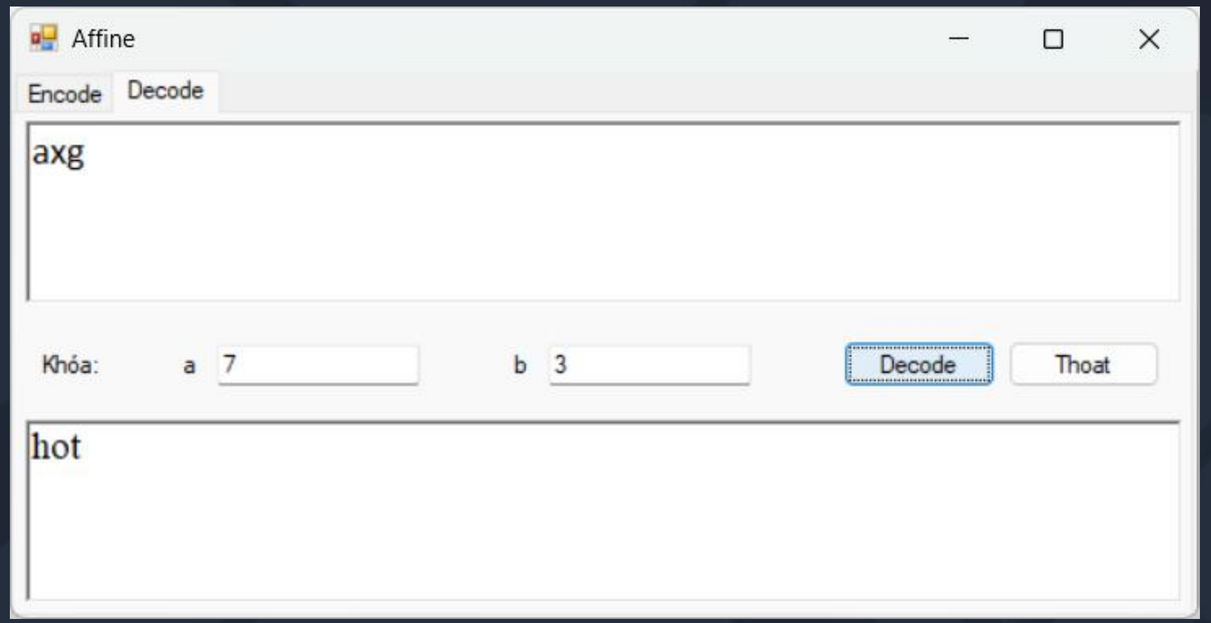
Hình 3. 1 Giao diện của chương trình

Ví dụ minh họa

Hình 3. 2 Mẫu thử mã hoá (1)

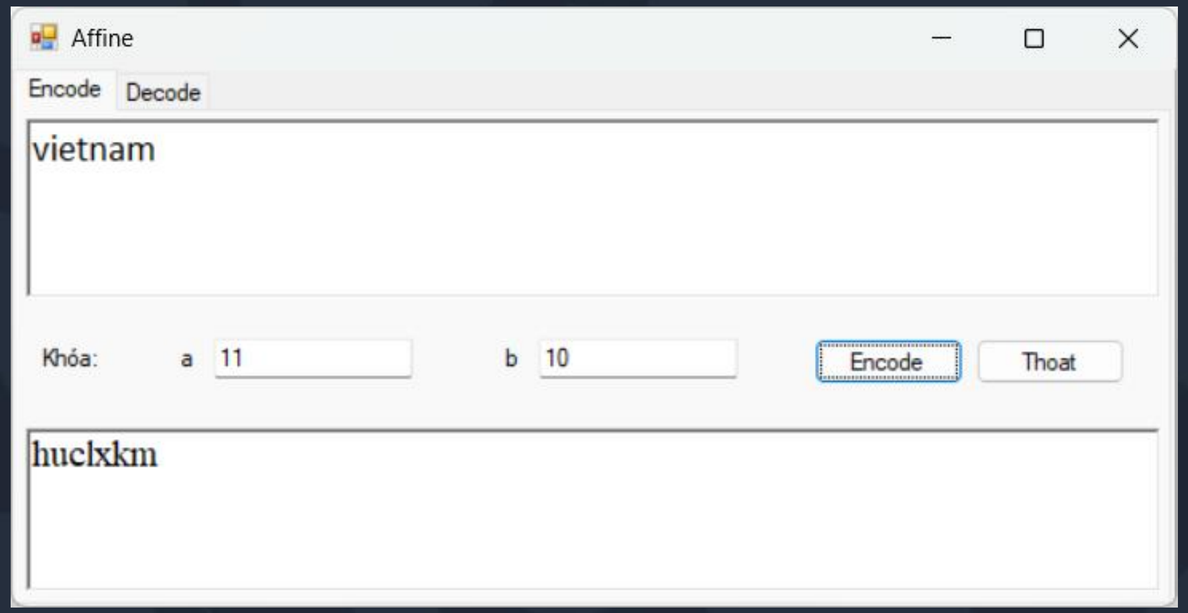


Hình 3. 3 Mẫu thử Giải mã (1)

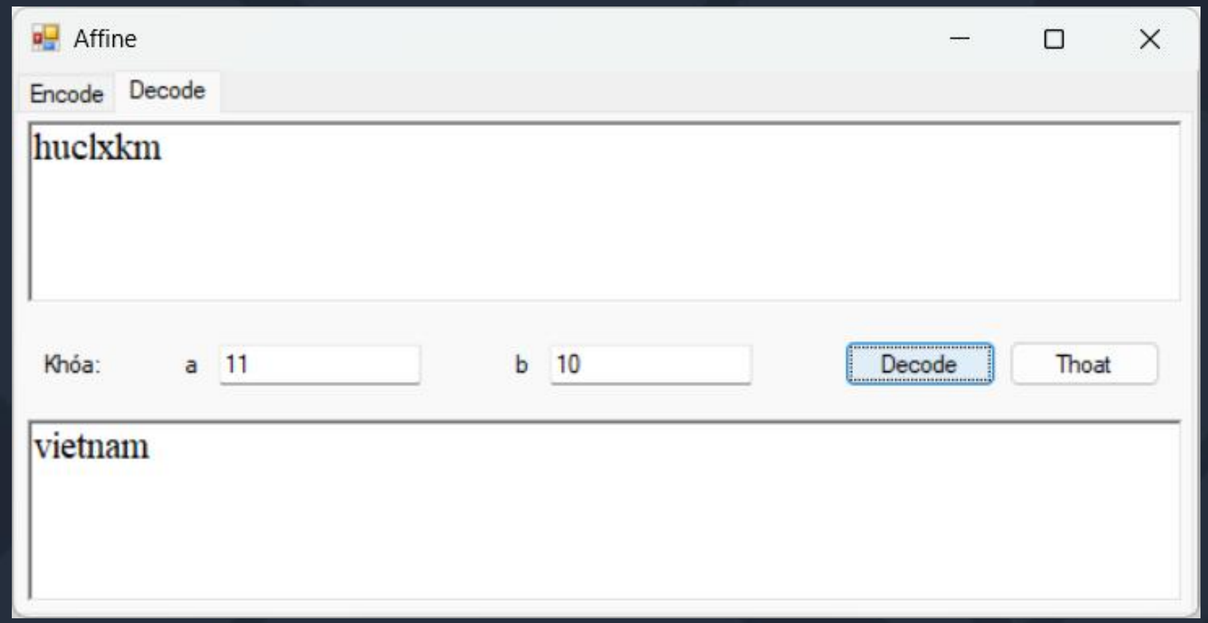


Ví dụ minh họa

Hình 3. 4 Mẫu thử Mã hoá (2)



Hình 3. 5 Mẫu thử Giải mã (2)



Nhóm 6

Học phần: An Toàn Bảo Mật Thông Tin

THANKS!