Cryptography

Eder Mazariegos

09/07/2017

1. Prove that encrypting a plaintext with two successive affine cipher keys is no more secure than encrypting a plaintext with a single set of affine cipher keys.

- If you encrypt using the Affine Cipher ax + b, and then proceed to encrypt using a separate key like dx + l, you would have…. D(AX + B) + L = (DA)X+ (DB + L), which would essentially give us the same function. So there is no more secure way to encrypting with two successive Affine Cipher keys.

1. Find 148-1 mod 327.

* 327 = 2\*148 + 31

148 = 31\*4 + 24

31 = 24\*1 + 7

24 = 7\*3 + 3

7 = 3\*2 + 1

1 = 7 – (3\*2)

3 = 24 – 21

1 = 7 – ((3) \*2)

1 = 7 – ((24 - 21) \*2)

1 = (31 - 24) – ((24 - 21) \*2)

1 = ((327 – (2\*148))- 24) – ((24 - 21) \*2)

148^-1(mod 327) = -2 = 325

or

2\*148 = 1 mod 327

148^-1 = 2 mod 327

1. For an alphabet of size 79, a set of affine encryption keys is a = 46, b = 22. (Thus the encryption function is f(x) = (46x + 22) % 79). Determine the corresponding set of decryption keys.

* 79 = 46\*1+33

46 = 33\*1+13

33= 13\*2+7

13= 7\*1+6

7 =6\*1+1

1 = 7 - (1\*6)

1 = 7 - (1\*(13-7))

1= 7\*2 – 13\*1

1= 2(33-(2\*13)) – 13\*1

1= 33\*2 - 13\*5 – 13\*1

1= 33\*2 – 13\*5

1= 33\*2 -5(46-33\*1)

1= 33\*2 – 33\*7 – 46\*5

1= (79-46)7 – 46\*5

1 mod 79 = 79\*7 – 12\*46

1 mod 79 = 46\*12

12 mod 79 = 46^-1

A^-1 = (Y-B) % 79

12 mod 79 = ((46x + 22%79) - 22) %79

1. A set of letters consists of 20 As, 35 Bs, 40 Cs, 5 Ds, 10 Es, and 50 Fs. What is the index of coincidence of the set?

20 A

35 B

40 C

5 D

10 E

50 F +

160 = x

(20/160) + (35/160) + (40/160) + (5/160) + (10/160) + (50/160) = (160/160) = 1

1. The set of letters S consists of 15 As, 25 Bs, 35 Cs, 15 Ds, and 10 Es. The set of letters T consists of 60 As, 25 Bs, 15 Cs, 20 Ds and 40 Es. What is the mutual index of coincidence between sets S and T? Leave your answer as a fraction in lowest terms.

|  |  |
| --- | --- |
| **S** | **T** |
| 15 A | 60 A |
| 25 B | 25 B |
| 35 C | 15 C |
| 15 D | 20 D |
| 10 E | 40 E |
| += 100 | += 160 |

(15/100 \* 60/160) + (25/100 \* 25/160) + (35/100 \* 15/160) + (15/100 \* 20/160) + (10/100 \* 40/160) =

(9/160) + (5/128) + (21/640) + (3/160) + (1/40) = 11/64

1. Encrypt the plaintext "FOOTBALLGAMEONTHURSDAY" using the Vigenere cipher and the keyword "KNIGHTS". (For practice for the first exam, do this by hand with a chart with the values of the letters.)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| K | N | I | G | H | T | S |
| 10 | 13 | 8 | 6 | 7 | 19 | 18 |

F = (5 + 10) % 26 = 15 | P

O = (14 + 13) % 26 = 1 | B

O = (14 + 8) % 26 = 22 | W

T = (14 + 6) % 26 = 25 | Z

B = (1 + 7) % 26 = 8 | I

A = (0 + 19) % 26 = 19 | T

L = (11 + 18) % 26 = 3 | D

L = (11 + 10) % 26 = 21 | V

G = (6 + 13) % 26 = 19 | T

A = (0 + 8) % 26 = 8 | I

M = (12 + 6) % 26 = 18 | S

E = (4 + 7) % 26 = 11 | L

O = (14 + 1) % 26 = 7 | H

N = (13 + 18) % 26 = 5 | F

T = (19 + 10) % 26 = 3 | D

H = (7 + 13) % 26 = 20 | U

U = (20 + 8) % 26 = 2 | C

R = (17 + 6) % 26 = 23 | X

S = (18 + 7) % 26 = 25 | Z

D = (3 + 19) % 26 = 22 | W

A = (0 + 18) % 26 = 18 | S

Y = (24 + 10) % 26 = 8 | I

1. Encrypt the message, "WHENWALLSCOMEDOWNEVERYONEWINS" using the Playfair cipher with the key "BRICKS" and the padding character "X". (Please do NOT use a program to do this.)

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

* Apply rules to encrypt through the square matrix…

Plaintext: WH\_EN\_WA\_LX\_LS\_CO\_ME\_DO\_WN\_EV\_ER\_YO\_NE\_WI\_NS

Encryption: RP\_FM\_RH\_QI\_GD\_BT\_TM\_SQ\_ZH\_SY\_AC\_VT\_MF\_XR\_GF

1. Decrypt the message, “ABEPCLCFWNAMNX”, which was enciphered using the Playfair cipher with the key “TURTLES”. Note: The padding character used was “Q”. (Please do NOT use a program to do this.)

* Apply the reverse method for decryption…

Encryption: AB\_EP\_CL\_CF\_WN\_AM\_NX

Decryption: SA\_LQ\_LY\_SI\_NG\_SN\_OW

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

Padding: “Q”

Key: “TURTLES”