Q1

confidentiality - protect sensitive information from unauthorized access

integrity - protect from unauthorized modification

availability - ensure timely and reliable access to information

Q2.

$A_1 = 1735$, $B_1 = 975$, $C_1 = 1$

$A_2 = 760$, $B_2 = 975$, $C_2 = 1$

$A_3 = 380$, $B_3 = 975$, $C_3 = 1$

$A_4 = 190$, $B_4 = 975$, $C_4 = 1$

$A_5 = 95$, $B_5 = 975$, $C_5 = 1$

$A_6 = 880$, $B_6 = 95$, $C_6 = 1$

$A_7 = 440$ .....

$A_8 = 220$ ...

$A_9 = 110$ ....

$A_{10} = 55$, $B_{10} = 95$, $C_{10} = 1$

$A_{11} = 40$, $B_{11} = 55$, $C_{11} = 1$

$A_{12} = 20$ ...

$A_{13} = 10$ ....

$A_{14} = 5$, $B_{14} = 55$, $C_{14} = 1$

$A_{15} = 50$, $B_{15} = 5$, $C_{15} = 1$

$A_{16} = 25$, $B_{16} = 5$, $C_{16} = 1$

$A_{17} = 20$, $B_{17} = 5$, $C_{17} = 1$

$A_{18} = 10$ $B_{18} = 5$ $C_{18} = 1$

$A_{19} = 5$ $B_{19} = 5$ $C_{19} = 1$

$GCD(1735, 975) = 5 \times 1 = 5$

Q3

| $a$ | 3 | 5 | 7 |
|---|---|---|---|
| $a^{-1} \bmod 23$ | 8 | 14 | 10 |

| $a$ | 5 |
|---|---|
| $a^{-1} \bmod 22$ | 9 |

| $a = 5^{\text{dlog}_{5,23} a} \bmod 23$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $\text{dlog}_{5,23} a$ | 0 | 2 | 10 | 4 | 1 | 18 | 19 | 6 | 10 | 3 | 9 | 20 | 14 | 21 | 17 | 8 | 7 | 12 | 15 | 5 | 13 | 11 |

(a)

$$X^5 \equiv 3^{-1} \cdot 2 \bmod 23 \equiv 16 \bmod 23 \equiv 5^8 \bmod 23$$

$$5\,\text{dlog}_{5,23} X \equiv 8 \bmod 22$$

$$\text{dlog}_{5,23} X \equiv 72 \bmod 22 \equiv 6 \bmod 22$$

$$X \equiv 8 \bmod 23$$

(b)

$$7X^{10} \equiv 22 \bmod 23$$

$$X^{10} \equiv 7^{-1} \cdot 22 \bmod 23 \equiv 220 \bmod 23 \equiv 13 \bmod 23 \equiv 5^{14} \bmod 23$$

$$10\,\text{dlog}_{5,23} X \equiv 14 \bmod 22$$

$$5\,\text{dlog}_{5,23} X \equiv 7 \bmod 11, \quad \text{dlog}_{5,23} X \equiv 5^{-1} \cdot 7 \bmod 11 \equiv 63 \bmod 11 \equiv 8 \bmod 11$$

$$\text{dlog}_{5,23} X \equiv 8 \bmod 22 \text{ or } 19 \bmod 22$$

$$X \equiv 16 \bmod 23 \text{ or } 7 \bmod 23$$

(c)

$$5^X \equiv 5^{18} \bmod 23$$

$$X \equiv 18 \bmod 22$$

Q 4

(a)

IO → MA
nl → PA
yr → ZO
eg → QH
re → GJ
tx → HW
th → HM
at → LI
Ih → TM
av → IA
eb → JH
ut → PB
on → AS
el → DG
iv → CA
et → DH
og → RO
iv → CA
ef → FJ
or → RA
my → FO
co → FA
un → NP
tr → BD
yg → ZV

(b)

IO → MA
nl → PA
yr → ZO
eg → QH
re → GJ
tx → HW
th → HM
at → LI
Ih → TM
av → IA
eb → JH
ut → PB
on → AS
el → DG
iv → CA
et → DH
og → RO
iv → CA
ef → FJ
or → RA
my → FO
co → FA
un → NP
tr → BL
yg → ZV

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

(a) and (b)

$C_a = C_b$ : MAPAZOQHGJHWHMLITMIAJHPBASDGCADHROCAFJRAFOFANPBDZV

(c)

the encrypt results won't be changed by column or row shifts of the matrix.

Q5.

a. $A = \begin{pmatrix} 1 & 3 \\ 1 & 22 \end{pmatrix}$

$A^{-1} = \frac{1}{\begin{vmatrix} 1 & 3 \\ 1 & 22 \end{vmatrix}} \begin{pmatrix} 22 & -3 \\ -1 & 1 \end{pmatrix}$ , $\begin{vmatrix} 1 & 3 \\ 1 & 22 \end{vmatrix} = 41 \equiv 15 \bmod 26$ , $41^{-1} = 7$

$A^{-1} = 7 \begin{pmatrix} 22 & -3 \\ -1 & 1 \end{pmatrix} \bmod 26$

$26 = 15(1) + 11$
$15 = 11(1) + 4$
$11 = 4(2) + 3$
$4 = 3(1) + 1$

$1 = 4 - 3$
$= 4 - 11 + 4(2)$
$= 4(3) - 11$
$= (15 - 11)(3) - 11$
$= 3(15) - 4(11)$
$= 3(15) - 4(26 - 15)$
$= 7(15) - 4(26)$

b. $B = \begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$

$\det(B) = \det \begin{pmatrix} 6 & 24 & 1 \\ -49 & -224 & 0 \\ -70 & -343 & 0 \end{pmatrix} = \det \begin{pmatrix} -49 & -224 \\ -70 & -343 \end{pmatrix} = 16121 - 13860$

$= 441 \equiv 25 \bmod 26$

$343 \times 41 = 2401 + 13720 = 16121$

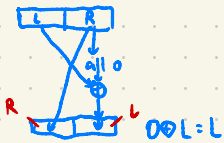
$70 \times 224 = 280 + 15680$

$25^{-1} \equiv 25 \pmod{26}$

$B^{-1} = 25 \begin{pmatrix} 70 & -343 & 224 \\ 5 & 70 & -49 \\ -99 & 378 & -216 \end{pmatrix}$

Q6.

a.




$L \oplus 0 = L$ , DES do 16 rounds , so the cybertext = plaintext

b.


3 個 1 條線 , equivelant to only doing 1 round → not strong enough

Q1

$(F, +, \times)$

① $(F, +, \times)$ → integral domain

({closure, identity element, associative, commutative} for + and ×, distributive law, inverse element for +)

②

multiplicatin inverse

satisfy ① and ② → $(F, +, \times)$ is a field

Q8

$(x^2+1)a \equiv 1 \mod x^3+x+1$

$x^3+x+1 = x(x^2+1) + 1$

$1 = x^3+x+1 - x(x^2+1)$

$a = X$

the multiplicative inverse $= X$