HomeWork N 20

N1a.

M = „DO NOT PASS GO"

K = 3. Formula $f(p) = (p+k) \mod 26$

D → 3 + K = 6 → G

O → 14 + K = 17 → R

N → 13 + K = 16 → Q

T → 19 + K = 22 → W

P → 15 + K = 18 → S

A → 0 + K = 3 → D

S → 18 + K = 21 → V

G → 6 + K = 9 → J

~~Encrypted M = GRQWSDVJ~~

Encrypted M = GRQRWSDVVJR

N4a.

Decrypt M = „EOXH MHDQV"

K = 3. Formula $f^{-1}(p) = (p-k) \mod 26$

E → 4 - 3 = 1 → B

O → 14 - 3 = 11 → L

X → 23 - 3 = 20 → U

H → 7 - 3 = 4 → E

M → 12 - 3 = 9 → J

D → 3 - 3 = 0 → A

Q → 16 - 3 = 13 → N

V → 21 - 3 =

Decrypted M =

N7.

Cryptanalatyze

NBOKW"

0 × 5, we ca

K = 10. Formu

D → 3 - 10 =

Y → 24 -

C → 2 -

V → 21 -

O → 14 -

Z → 25 -

B → 1 -

M → 12

R → 17

K → 1

X → 2

N →

W →

Decryp

TO

V → 21 - 3 = 18 → S

Decrypted M = „BLUE JEANS"

N7.

Cryptanalalyze M = „DY CWOOZ ZOBMRKXMO DY NBOKW"

D × 5, we can assume it's E then it ~~means~~ means 14-4 = 10

K=10. Formula $f^{-1}(p) = (p-k) \bmod 26$

D → 3-10 = -7 mod 26 → = 19 → T

Y → 24 -10 = 14 mod 26 → = O

C → 2 - 10 = -8 mod 26 = 18 → S

V → 21-10 = 11 → L

O → 14 - 10 = 4 → E

Z → 25 - 10 = 15 → P

B → 1 - 10 = -9 mod 26 = 17 → R

M → 12 - 10 = 2 → C

R → 17 - 10 = 7 → H

K → 10 - 10 = 0 → A

X → 23 - 10 = 13 → N

N → 13 - 10 = 3 → D

W → 22 - 10 = 12 → M

Decrypted M = „TO SLEEP ~~PER~~ PERCHANCE TO DREAM„

N11.

Decryption fun. for Affine Cipher

$c = (15p + 13) \bmod 26$,

1. To find modular inverse of a mod 26, mod inverse.

2. $p = \bar{a}(c - b) \bmod 26$

Formula, $f(p) = (ap + b) \bmod 26 \rightarrow a = 15$ and $b =$

1) Modular Inverse $ax \equiv 1 \bmod 26$

$15 \cdot 2 \equiv 4 \bmod 26$

$15 \cdot 4 \equiv 8 \bmod 26$

$15 \cdot 8 \equiv 16 \bmod 26$

$15 \cdot 11 \equiv 9 \bmod 26$

$15 \cdot 14 \equiv 2 \bmod 26$

} Picking

Extended Euclidean Algo.

$\gcd(a, m) \rightarrow a = 15, m = 26$

$sa + tm = \gcd(a, m) = 1$

$sa + tm = 1 \bmod m$

$s\,15 + 26t = 1 \bmod 26$

~~$2 \cdot 15 + 9 = 26$~~ ~~$1 \cdot 15 + 11 = 26$~~

~~$11 = 26 + (2 \cdot 15) = 11$~~

~~$11 = 26 +$~~ $1 \cdot 15 + 11 = 26 \Rightarrow 26 - (1 \cdot 15) = 11$

~~$11 = 26 +$~~ $1 \cdot 11 + 4 = 15 \Rightarrow 15 - (1 \cdot 11) = 4$

$2 \cdot 4 + 3 = 11 \Rightarrow 11 - (2 \cdot 4) = 3$

~~$3 \cdot 3 + 2 = 11$~~ $1 \cdot 3 + 1 = 4 \Rightarrow (4) - (1 \cdot 3) = 1$

~~$4 =$~~ $\bar{a} = 7$

2) $p =$

$p = (7c -$

$p = (7c -$

$p = (7c$

N24.

Encrypt

A → 00

T → 19

C → 02

K → 10

$M_1 = 19$

$M_2 = 1$

$M_3 = 21$

$C_1 = 1$

$C_2 = 1$

$C_3 =$

Ciphe

N29.

Diff

Publi

Alic

Bo

inverse - $\bar{a}$

ed $\beta = 13$

2) $p = 7(c - 13) \mod 26$

$p = (7c - 7 \cdot 13) \mod 26$

$p = (7c - 91) \mod 26$

$p = (7c + 13) \mod 26$ or $p = 7(c - 13) \mod 26$

N24.

Encrypt M_{11} "ATTACK" using RSA $\rightarrow n = 43 \cdot 59$, $e = 13$

A → 00

T → 19

C → 02

K → 10

$M_1 = 19$ (AT) → 0019 → 19

$M_2 = 1900$ (TA) → 1900

$M_3 = 210$ (CK) → 0210 → 210

$C_1 = 19^{13} \mod 2537 = 1819$

$C_2 = 1900^{13} \mod 2537 = 1415$

$C_3 = 210^{13} \mod 2537 = 0981$

Ciphertext: 1819 1415 0981

N29

Diffie-Hellman. $p = 23$, $a = 5$, $k_1 = 8$, $k_2 = 5$.

Public keys, $p = 23$ and $a = 5$

Alice - $K_1 = 8$

Bob - $K_2 = 5$

Alice:

$A = a^{k_1} \mod p = 5^8 \mod 23$

$5^8 = 390625$

$390625 \mod 23 = 16$

Bob:

$B = a^{k_2} \mod p \rightarrow 5^5 \mod 23$

$5^5 = 3125$

$3125 \mod 23 = 20$

$A = 16 \quad B = 20$

sAlice $= B^{k_1} \mod p \rightarrow 20^8 \mod 23 \rightarrow 18$

sBob $= A^{k_2} \mod p \rightarrow 16^5 \mod 23 \rightarrow 18$

$S = 18.$