Date
Page

Assignment 2

Vigenere Cipher

1. A cipher text is suspected to have been encrypted using the Vigenere Cipher. Describe and demonstrate how the Kasiski Examination method can be used for encryption

Ans: The Kasiski Examination is a cryptographic method used to estimate the length of the key in a Vigenere Cipher. The vigenere cipher is a polyalphabetic cipher that uses a keyword to determine the shifting of each letter in the plain text. The kasiski help identify repeated patterns in the cipher text thereby revealing the key

Steps in Kasiski Examination.

1. Identify Repeated Sequences: ~~Scan~~ Search the cipher text for repeated sequences of letters
2. Measure Distances: Note the distances between the starting points of these repeated sequences
3. Find common factors: Determine the greatest common divisor (GCD) of these distances.

Example:

Ciphertext: ZICVTWQNGRZGVTWAVZHCQYG
LMGJ

Repeated sequence: "VTW" at position 3 and 10.

Distance: 10 − 3 = 7

GCD: If distances are 7, 14, 21
then GCD(7, 14, 21) = 7
Likely key = 7

02 Cipher Text: KSMEHZBBLKSMEMW
Plain Text: SECRETMESSAGE

Row:- KSMEHZBBLKSMEMW
SECRETMESSAGESE

$C = P + k \mod 26$

$k = C - P \mod 26$

K = 10

S = 18

$k = 10 - 18 \mod 26 = -8 \mod 26 = 18 = S$

S-E 18 - 4 mod 26 = 14 = O

M-C 12 - 2 mod 26 = 10 = K

E-R 4 - 17 mod 26 = 13 = N

H-E 7 - 4 mod 26 = 3 = D

Z-T 25 - 19 mod 26 = 6 = G

B-M 1 - 12 mod 26 = 15 = P

B-E 1 - 4 mod 26 = 23 = X

L-S 11 - 18 mod 26 = 19 = T

K-S 10 - 18 mod 26 = 18 = S

S-A 18 - 0 mod 26 = 18 = S

M-G 12 - 6 mod 26 = 6 = G

E-E 4 - 4 mod 26 = 0 = A

The key is

Q3) Cipher text: U2QSQVU04XMOPVGPO2PGVSG,ZWSZOP

F.PESXUDBMET.SXAIZ

describe how frequency analysis can help break the cipher if the key length is already known to be 5

Spliting the cipher text into groups based on the key length

Group 1 → Position → (1, 6, 11, 16, 21, 26 ---) → U, O, X, P ---

Group 2 → Position → (2, 7, 12, 17, 22, 27, 32, 37, 42) → Z, V, O, V, P ---

Group 3 → Position → (3, 8, 13, 18, 23, 28, 33, 38, 43) → Q, U, 4, G, E ---

Group 4 → Position → (4, 9, 14, 19, 24, 29, 34, 39, 44) → S, O, M, P, S ---

Group 5 → Position → (5, 10, 15, 20, 25, 30, 35, 40, 45) → O, U, O, V, ...

Analyse frequency of each letter in each group

Group 1 → U:1, O:1, X:2, P:1, Z:1, G:1, D:1 → X appears 2 times
Group 2 → Z:2, V:2, O:1, P:1, M:1, E:1 → Z & V both appear 2 times
Group 3 → Q:1, U:1, H:1, G:1, E:1, S:1, B:1, T:1 → No Repetition
Group 4 → S:3, O:1, M:1, P:1, W:1, E:1 → S appears 3 times
Group 5 → O:2, U:1, V:2, Z:1, T:1, A:1 → O & V both appear 2 times

Group 1 : The most frequent letter is "X"
Shift = X − E = 23 − 4 = 19 (T)
Group 2: The most frequent letters are "Z" & "V"
Shift "Z" = Z − E = 25 − 4 = 21 (V)
Shift "V" = V − E = 17 (R)
Group 3: Let's assume ~~The most~~ frequent letter ~~are~~ is "S"
Shift = S − E = 18 − 4 = 14 (O)
Group 4: The most frequent letter is "S"
Shift = S − E = 18 − 4 = 14 (O)
Group 5 : The most frequent letter is "O"
Shift = O − E = 14 − 4 = 10 (K)

∴ key : T, V, O, O, K
"TVOOK"

classmate
Date
Page

Vigenère cipher vs Caesar cipher

→ Caesar cipher: A monoalphabetic cipher with only 25 possible shifts, making it weak. It vulnerable to brute force and frequency analysis

→ Vigenere cipher: A ~~proto~~ poly alphabetic cipher that uses a repeating key. Its strength increases with key length. A short key is vulnerable to frequency analysis, while long key is much stronger. Shortkey length weakens the vigenère cipher because key repetition makes it vulnerab -le. Improves security, and a key as long as the message provides perfect security

Exploiting key length:

⇒ Attackers can split cipher text into grou -ps based on the keys length and use freq -uency analysis to deduce the key. For ⇒ short key, attackers can try all possible combinations. If the key length is unkn -own, attackers can use repeated sequen -ces in the cipher text to estimate it

Affine Cipher:

01/ cipher key = (7, 17)

$0 \leq r \; ; \; s \leq 25$

$d_k(y) = ry + s$

$e_k(x) = (a \times x + b) \bmod 26$

$a = 7, \; b = 17$

$d_k(y) = a^{-1} \times (y - b) \bmod 26$

$a \times a^{-1} \equiv 1 \pmod{26}$

$\boxed{a = 7}$ $\quad 7 \times 15 = 105 \equiv 1 \pmod{26}$

$a^{-1} = 15$ & $b = 17$ (substitution in decryption formula)

$d_k(y) = 15 \times (y - 17) \bmod 26$

$d_k(y) = (15xy - 15 \times 17) \bmod 26$

$15 \times 17 = 255$ and $255 \bmod 26 = 21$

$d_k(y) = (15y - 21) \bmod 26$

$d_k(y) = rxy + s$

$d_k(y) = (15y + 26 - 21) \bmod 26$

$d_k(y) = (15y + 5) \bmod 26$

$r = 15$ & $s = 5$

Q2) $k = (11, 25)$

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

$d_k(x) = a^{-1}(y - b) \bmod 26$

$a \times a^{-1} \equiv 1 \pmod{26}$

$\boxed{a = 11}$ $\quad 11 \cdot a^{-1} \equiv 1 \pmod{26}$

$11 \cdot 19 = 209$ and $209 \bmod 26 = 1$

$\boxed{a^{-1} = 19}$ $\quad \boxed{b = 25}$

$d_k(y) = 19(y - 25) \bmod$

$d_k(y) = (19y - 475) \bmod 26$

$475 \bmod 26 = 7$

$d_k(y) = (19y - 7) \bmod 26$

$d_k(y) = ry + s$

$d_k(y) = 19y + 26 - 7) \bmod 26$

$d_k(y) = (19y + 19) \bmod 26$

$r = 19$ and $s = 19$

Q3) $e(x) = 3x + 10 \bmod 26$.

$d(y) = (cy + d) \bmod 26$ $[d(y) = a^{-1} \cdot (y - b) \bmod 26]$

cipher text: "VBHVCHQUBHAHOVVHXOLPUVO JRDK"

$a = 3, \; b = 10$.

$3 \cdot a^{-1} \equiv 1 \bmod 26$

$3 \cdot 9 = 27 \equiv 1 \pmod{26}$ $\quad a^{-1} = 9$

$d(y) = 9 \cdot (y - 10) \bmod 26$

$d(y) = (9y - 90) \bmod 26$

$d(y) = (9y + 18) \bmod 26$

V = (9x20+18) mod 26 = 16 (Q)
B = (9x1+18) mod 26 = 1 (B); H(7) = (9x7+18) mod 26 = 3 (D);
H(21) = (9x21+18) mod 26 = 25 (Z); L = (9x11+18) mod 26 = 13 (N)
G = (9x6+18) mod 26 = 20 (U); X = (9.23+18) mod 26 = 17 (R);
O = (9x14+18) mod 26 = 14 (O); D = (9x3+18) mod 26 = 19 (T);
P = (9x15+18) mod 26 = 23 (X); J = (9x9+18) mod 26 = 21 (V);
R = (9x17+18) mod 26 = 15 (P); K = (9x10+18) mod 26 = 4 (E)

Final plain text: "QBDZNDUQBDRDOZQDPTNXQZOVPTE"

Q4) $e(x) = (9x+3) \bmod 26$

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

$a = 9, \; b = 3$

$9 \cdot a^{-1} \equiv 1 \pmod{26}$

$9 \cdot 3 = 27 \equiv 1 \pmod{26}$

$a^{-1} = 3$

$d(y) = 3(y-3) \bmod 26$

$d(y) = (3y-9) \bmod 26$

$d(y) = (3y+17) \bmod 26$

S = (3x18+17) mod 26 = 19 (T)
A = (3x0+17) mod 26 = 17 (R)
B = (3x1+17) mod 26 = 20 (U)
N = (3x13+17) mod 26 = 4 (E)

Plain Text: "TRUE"