Cryptology Packet Pt3

ID: 1747

January 2023

1. Using the Caesar Cipher, encrypt the message ATTACK AT DAWN.

   $C \equiv P + 3 \mod 26$
   A= $0 + 3 \mod 26 = 3$=D
   T= $19 + 3 \mod 26 = 22$=W
   T= $19 + 3 \mod 26 = 22$=W
   A= $0 + 3 \mod 26 = 3$=D
   C= $2 + 3 \mod 26 = 3$=F
   K= $10 + 3 \mod 26 = 13$=N
   A= $0 + 3 \mod 26 = 3$=D
   T= $19 + 3 \mod 26 = 22$=W
   D= $3 + 3 \mod 26 = 6$=G
   A= $0 + 3 \mod 26 = 3$=D
   W= $22 + 3 \mod 26 = 25$=Z
   N= $13 + 3 \mod 26 = 16$=Q
   So ATTACK AT DAWN becomes DWWDFN DW GDZQ

2. Decrypt the ciphertext message LFDPH LVDZL FRQTX HUHG, which has been encrypted using the Caesar Cipher.

   $C \equiv P + 3 \mod 26$
   $P = (C - 3) \mod 26$

   L=$(11 - 3) \mod 26 = 17$ =I
   F=$(5 - 3) \mod 26 = 2$ =C
   D=$(3 - 3) \mod 26 = 0$ =A
   P=$(15 - 3) \mod 26 = 12$ =M
   H=$(7 - 3) \mod 26 = 4$ =E
   L=$(11 - 3) \mod 26 = 17$ =I
   V=$(21 - 3) \mod 26 = 18$ =S
   D=$(3 - 3) \mod 26 = 0$ =A
   Z=$(25 - 3) \mod 26 = 22$ =W
   L=$(11 - 3) \mod 26 = 17$ =I
   F=$(5 - 3) \mod 26 = 2$ =C
   R=$(17 - 3) \mod 26 = 14$ =O

Q=$(16-3) \mod 26 = 13$ =N
T=$(19-3) \mod 26 = 16$ =Q
X=$(23-3) \mod 26 = 20$ =U
H=$(7-3) \mod 26 = 4$ =E
U=$(20-3) \mod 26 = 17$ =R
H=$(7-3) \mod 26 = 4$ =E
G=$(6-3) \mod 26 = 3$ =D

Translated, it becomes ICAME ISAWI CONQU ERED

3. Encrypt the message SURRENDER IMMEDIATELY using the affine transformation $C \equiv 11P + 18 \mod 26$

S= $11 * 18 + 18 \mod 26 = 8$=I
U= $11 * 20 + 18 \mod 26 = 4$=E
R= $11 * 17 + 18 \mod 26 = 23$=X
R= $11 * 17 + 18 \mod 26 = 23$=X
E= $11 * 4 + 18 \mod 26 = 10$=K
N= $11 * 13 + 18 \mod 26 = 5$=F
D=$11 * 3 + 18 \mod 26 = 25$=Z
E= $11 * 4 + 18 \mod 26 = 10$=K
R= $11 * 17 + 18 \mod 26 = 23$=X
I= $11 * 8 + 18 \mod 26 = 2$=B
M= $11 * 12 + 18 \mod 26 = 20$=U
M= $11 * 12 + 18 \mod 26 = 20$=U
E= $11 * 4 + 18 \mod 26 = 10$=K
D=$11 * 3 + 18 \mod 26 = 25$=Z
I= $11 * 8 + 18 \mod 26 = 2$=B
A= $11 * 0 + 18 \mod 26 = 18$=S
T= $11 * 19 + 18 \mod 26 = 19$=T
E= $11 * 4 + 18 \mod 26 = 10$=K
L= $11 * 11 + 18 \mod 26 = 9$=J
Y= $11 * 24 + 18 \mod 26 = 22$=W

So, this encrypts to IEXXKFZKX BUUKZBSTKJW

4. Decrypt the message YLFQX PCRIT, which has been encrypted using the affine transformation $C \equiv 21P + 5 \mod 26$

$c = aP + b \mod 26$
$P = a^{-1}(C - b) \mod 26$
$a^{-1} \mod 26 = 21^{-1} \mod 26 \equiv 5$
$P = 5(C - 5) \mod 26$
Y=$5(24 - 5) \mod 26 = 17$ =R
L=$5(11 - 5) \mod 26 = 4$ =E
F=$5(5 - 5) \mod 26 = 0$ =A
Q=$5(16 - 5) \mod 26 = 3$ =D

X=$5(23-5) \mod 26 = 12$ =M
P=$5(15-5) \mod 26 = 24$ =Y
C=$5(2-5) \mod 26 = 11$ =L
R=$5(17-5) \mod 26 = 8$ =I
I=$5(8-5) \mod 26 = 15$ =P
T=$5(19-5) \mod 26 = 18$ =S

So, this decrypts to READM YLIPS

5. If the most common letter in a long cipher text, encrypted by a shift transformation $C \equiv P+k \mod 26$ is Q, then what is the most likely value of k?

   The most common letter is E so $P = E = 4$. We can find how much k is by finding the amount needed to get Q(16) which is $16 - 4 = 12$. So, $C \equiv P + 12 \mod 26$.

6. The message IVQLM IQATQ SMIKP QTLVW VMQAJ MBBMZ BPIVG WCZWE VNZWU KPQVM AMNWZ BCVMK WWSQM was encrypted by a shift transformation $C \equiv P + k \mod 26$. Use frequencies of letters to determine the value of k. What is the plain text message?

   Since we know that E is the most common letter in the alphabet, we can find the most common letter in the cipher text which is M. So, $k = 8$ since $12 \equiv 4 + 8 \mod 26$.

   Therefore, the message will shift by 8 and the plain text will be ANIDE AISLI KEACH ILDNO NEISB ETTER THANY OUROW NFROM CHINE SEFOR TUNEC OOKIE.

7. If the two most common letters in a long cipher text, encrypted by an affine transformation $C \equiv aP + b \mod 26$, are W and B, respectively, then what are the most likely values for a and b?

   The most common letters in English are E and T respectively. If W decrypts in plain text to E and B decrypts to T then we can think of the affine transformation as a linear function. We can use the decryption index as the x-coordinate and the encryption index as the y-coordinate so the coordinate points would be $(4, 22)$ and $(19, 27)$. Note that instead of using the encryption index of B as 1, we can use it as 27 since it is mod 26 to find a linear function. We find that $C \equiv 0.33P + 20.67 \mod 26$ where $a = 0.33$ and $b = 20.67$

   $a' \equiv a^{-1} \mod 26$
   $0.33 \equiv a^{-1} \mod 26$
   $0.33a \equiv 1 \mod 26$
   0.33 is an inverse of 3, 9 is also an inverse of 3 so we can substitute 0.33 with 9.

$a = 9$

$C \equiv 9P + b \mod 26$
$22 \equiv 9 * 4 + b \mod 26$
$36 + b \mod 26 \equiv 22$
$b = 12$

$C \equiv 9P + 12 \mod 26$

8. The message WEZBF TBBNJ THNBT ADZQE TGTYR BZAJN ANOOZ ATWGN ABOVG FNWZV A was encrypted by an affine transformation $C \equiv aP + b \mod 26$. The most common letters in the plain text are A, E, N, and S. What is the plain text message?

   Consider the case where the encoded letters A, B, T, and N are decoded as N, S, E, and A respectively.
   $0 \equiv a * 13 + b \mod 26$
   $b = 13$
   $1 \equiv a * 18 + 13 \mod 26$
   $21 * 18 + 13 \mod 26 \equiv 1$
   $a = 21$

   Using the decryption algorithm: $P = a^{-1}(C - b) \mod 26$, $P = 21^{-1}(C - 13) \mod 26$. The plain text message will be THISM ESSAG EWASE NCIPH EREDU SINGA NAFFI NETRA NSFOR MATIO N.

9. Given two ciphers, plaintext may be encrypted by first using one cipher, and then using another cipher on the result. This procedure produces a *product cipher*. Find the product cipher obtained by using the transformation $C \equiv 5P + 13 \mod 26$ followed by the transformation $C \equiv 17P + 3 \mod 26$

   $C \equiv 17(5P + 13) + 3 \mod 26$
   $C \equiv 85P + 221 + 3 \mod 26$
   $C \equiv 85P + 224 \mod 26$
   $C \equiv 7P + 16 \mod 26$