암호학개론 HW#1 20191629 이주호

Chapter 3

18. What is the maximum # of characters that will be changed if one character is changed in plaintext?

a. Additive : ith ciphertext C_i only depends on the i^{th} plaintext.
→ Only 1 character

b. Multiplicative : Same as additive, but using multiplication.
→ Only 1 character

c. Affine : Combination of additive and multiplicative.
→ Only 1 character

d. Vignere : i^{th} Ciphertext C_i depends on i^{th} plaintext P_i and i^{th} key k_i. k_i remains constant.
→ Only 1 character

e. Auto-key : It is a Vignere cipher when $k_i = P_{i-1}$. Therefore, C_i and C_{i+1} are diffbent, as they are given by $P_i + P_{i-1} \pmod{26}$ and $P_{i+1} + P_i \pmod{26}$.
→ 1 if the last character is changed, 2 otherwise

f. One-time pad: It is a Vignere cipher with a key length equal to the plaintext length.
→ Only 1 character

19. What is the maximum # of characters that will be changed if one character is changed in plaintext?

a. Single transposition. it is a Transpositional cipher.
→ Only 1 character.

b. Double transposition: it is also a transpositional cipher.
→ Only 1 character

27. a. Eve is launching a chosen-plaintext attack.

b. Length of "abcdefghij" is 10. Divisors of 10 are: 1. 2. 5. 10.

As breaking with key = 1 or 10 would be trivial, the permutation key length is 2 or 5.

29. Use bruteforce attack. plaintext "ab" is known to cipher into "GL", and affine cipher is used.

$a(00) \rightarrow G(06)$, $b(01) \rightarrow L(11)$.

Thus, $\begin{cases} 0 \cdot k_1 + k_2 \equiv 06 \pmod{26} \\ 1 \cdot k_1 + k_2 \equiv 11 \pmod{26} \end{cases} \Rightarrow k_2 = 6,\ k_1 = 5.$

To compute plaintext,

$$P_i = \left(\frac{C_i - 6}{5}\right) \pmod{26} = \left(21\,(C+20)\right) \pmod{26}$$

X P A L A S X Y F G F U K P X U S O G E U T K C D G F X A N M G N V S
t h e b e s t o f a f i g h t i s m a k i n g u p a f t e r w a r d s

→ The best of a fight is making up afterwards.

31. Assume punctuations are added, making $\mathbb{Z}_{29}$ space.

a. Each entry can contain 29 letters. $29 \times 29 \times 29 \times 29 = \boxed{707281}$ matrices.

b. Hill cipher requires invertible matrix to decode. Thus:

$$(29^2 - 1)(29^2 - 29) = 840 \cdot 812 = \boxed{682080}$$ key matrices.

39. Suppose the plaintext is an identity matrix for a Hill cipher.

For arbitrary matrix A, $A \cdot I = I \cdot A = A$.

Thus, from a Hill cipher, $C = P \cdot K$, the identity $P = I$ gives:

$$C = I \cdot K = K,$$

the ciphertext "is" the key.

Hence, suppose Eve gains access to Alice's device and launches a chosen-plaintext attack with identity input, Eve can trivially retrieve Alice's key.