2019 1583 김태균

18.

(a) In additive cipher, $C_i = (P_i + k) \bmod 26$. When one plaintext character is changed, one cipher character is changed. C_i only depends on P_i

(b) In multiplicative cipher, $C_i = (P_i \times k) \bmod 26$. when one plaintext character is changed, one cipher character is changed. C_i only depends on P_i

(c) In affine cipher, $C_i = (P_i \times k_1 + k_2) \bmod 26$. when one plaintext character is changed one cipher character is changed. C_i only depends on P_i

(d) In Vigenere cipher, $C_i = (P_i + k_i) \bmod 26$. The value of k can change, but the change does not depend on the previous or next character. The change depends only on the position of the plain text character. So when one plcintext character is changed, one cipher character is changed.

(e) In autokey cipher, $C_i = (P_i + k_i) \bmod 26 = (P_i + P_{i-1}) \bmod 26$. Each ciphertext character depends on its corresponding plaintext character and previous plaintext character. So, changing just one character in the plaintext changes all ciphertext characters after that character.

(f) In one-time pad, the key stream used only once. The ciphertext character depends on plain text character, so when one plaintext character is changed, one ciphertext character is changed.

19.

(a) Single transposition only reorders the characters. when one plaintext Chacrater is Changed, one Ciphertext character is changed.

(b) Double transposition only reorders the characters, when one plaintext character is changed, one Ciphertext character is changed.

20.

(a) Chosen-ciphertext attack

(b) The message length is 10. So The number of colums can 1, 2, 5, 10. But, if the size of permutation key is 1, all characters remain intact.
If the permutation key size is 10, then any transformation is possible, so it makes more sense to find a smaller key size that only allows certain transformations
Therefore, the number of colums is either 2 or 5.

29.

a	b	c	d	···
$\boxed{0}$	$\boxed{1}$	2	3	···

A	B	C	D	E	F	G	H	I	J	K	L
0	1	2	3	4	5	$\boxed{6}$	7	8	9	10	$\boxed{11}$

a→G 00→06 b→L 01→11

$P \times k_1 + k_2 \equiv C \bmod 26 \Rightarrow \left.\begin{array}{l} 00 \times k_1 + k_2 \equiv 06 \bmod 26 \\ 01 \times k_1 + k_2 \equiv 11 \bmod 26 \end{array}\right) \Rightarrow \begin{array}{l} k_1 = 5 \\ k_2 = 6 \end{array}$

$P = ((C - k_2) \times k_1^{-1}) \bmod 26 \Rightarrow P = ((C-6) \times 5^{-1}) \bmod 26 \Rightarrow P = ((C+20) \times 21) \bmod 26$

⇒ the best of a fight is making up afterwards.

31.

(a) We can use 29 characters by ,.?.-

Since it is a 2x2 matrix, there are tatal of 29^4 possible cases.

$29^4 = 707281$

(b) $(N^2-1)(N^2-N) = (29^2-1)(29^2-29) = 682080$

39. In the Hill cipher, C=PK. When P is identity matrix I, then we have C=K

That is, if we have access to Alice's computer and a chosen-plaintext attack is possible, we can easily find the key. Hill cipher is vulnerable to chosen-plaintext attack.