U19CS012

3> n bit (n=128 bit) → $[1.12 \times (e^{36})]$

$\frac{(128)!}{(50!)(78!)}$

Attacker = 50 numbers → 1's
128 - 50 = 78 0's
(BRUTE force)

a) Substitution cipher [replace plain text →

① we can do frequency analysis of block (cipher) letter

① 1-to-1 unique mapping
② frequency of letters in english language
③ ~~tongue~~

(2^{50}) combination (finite time)

It does not change the number of 1's (can be cracked)

b) permutation cipher

try out all the permutation of all letters of alphabet
&
convert it into binary & then use it as dictionary to decrypt the cipher

It's same as substitution cipher, since permutations are not increasing (1's)

c) combination of subs + permutation cipher

~~It very hard to~~ Same ⇒ $\frac{(128)!}{50!78!}$ } (same time taken)

substitution → permutation → (no extra calc needed)