1. Show with a counterexample that the Substitution Cipher doesn't provide perfect secrecy.

PLAINTEXT: THE QUICK BROWN FOX.

CIPHERTEXT: QEB NRFZH YOLTK CLU

only ~~twice~~ 26 different combination that need to be checked.

test case: SIF

A → B ~~SWF~~ RVJ DL CSPXO GPY ← not decrypted

NO SECRECY

⋮

A → D ~~THE CAVE~~ THE QUICK BROWN FOX

2.

M = Plaintext P_1, P_2 = one-time pads C = ciphertext

$C = M \oplus P_1 \oplus P_2$

↑ ciphertext

One time pad is perfectly secret, because combination is used once.

Given:

M = 101101

P_1 = 001001

P_2 = 100100

Alice encrypts:

$C \rightarrow M \oplus P_1 \oplus P_2$

M → 101101

P_1 → 001001

100100

P2 → 100100

C → 000000

Bob Decrypts:

$D(C) = C \oplus P_1 \oplus P_2$

C → 000000

P_1 → 001001

001001

P_2 → 100100

M → 101101 ✓ ← successfully decrepted ✓

Eve cannot intercept the message unless she knows both pads.

(3.)

1. If an attacker knows a plaintext / cipher pair, they will know what is stored in the database when they see an encrypted cipher.
   ↳ Ex: Eve has data in database that they have diabetes. Eve knows the cipher ~~pair~~ text for the diabetes plaintext, and can identify which other people have diabetes.
2. Each ~~cipher~~ plaintext is encrypted with the same key. If the key is known all cipher text can be decrypted.