

② one-time-pad of a key that has
51% of 1's and 49% of 0's

Soln. Not Shannon-secure, $\cup \cup \cup \cup \cup$

let $m_1 = 111000$

$m_2 = 000111$

$C = 111000$

Then C is most-likely from m_2 .

③ Vigenere

P is 7 letters

K is ① 7 letters does not start X

② 7 unique letters ←

It is not perfect.

let $m_1 = \text{Hussain} \rightarrow x d t t$

$m_2 = \text{Abrahim}$

$C = a b \underline{k k} x y z$

Then C is must be from m_2
cannot be from m_1