

1) Proof: OTP has perfect secrecy

$$\textcircled{A} \cdot P_2[M=m|C=c] \stackrel{\text{BAYES LAW}}{=} P_2[C=c|M=m] \cdot \frac{P_2[M=m]}{P_2[C=c]}$$

Panko reminds:



$m \in \mathcal{M}$ } sets of messages
 $c \in \mathcal{C}$ } and cyphertexts
 M, C : random variables

$\forall m \in \mathcal{M}, P_2[M=m]$ a prior probability
 $K \in \mathcal{K}$

$$P_2[K=k] = \frac{1}{2^m} \text{ (m-bits)}$$

$$\mathcal{C}, \mathcal{M}, \mathcal{K} \in \{0,1\}^m$$

$$|\mathcal{C}| = |\mathcal{M}| = |\mathcal{K}|$$

$$\textcircled{1} P_2[C=c] \stackrel{\text{TOT PROB LAW}}{=}$$

$\hookrightarrow C$ can be generated from all messages. All messages form a partition



PANKO SAYS

$$\sum_s P_2[C=c|M=m_s] \cdot P_2[M=m_s] =$$

$$= \sum_s P_2[K=c \oplus m_s] P_2[M=m_s] = \sum_s \frac{1}{2^m} P_2[M=m_s] = \frac{1}{2^m} \sum_s P_2[M=m_s] = \frac{1}{2^m}$$

Assumption of 1TP

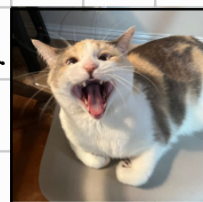
• Whatever is the message, the probability of having $C=c$ is $\frac{1}{2^m}$.

So, snap back:

$$\textcircled{A} P_2[M=m|C=c] = P_2[C=c|M=m] \cdot \frac{P_2[M=m]}{\frac{1}{2^m}}$$

② This probability is equal to the probability to have the key that encrypts m to c .
 We can say this because we know that the key to do this is unique.

PANKO ARGUES



$$\textcircled{A} P_2[M=m|C=c] = \frac{1}{2^m} \cdot \frac{P_2[M=m]}{\frac{1}{2^m}} = P_2[M=m] \quad \text{so one time pad is perfect.}$$