1) Proof: OTP has perfect secrecy

Panko reminds:

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

M, C: random variables

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

$k \in \mathcal{K}$

$Pr[K=k] = 1/2^n$ (n-bits)

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

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

(A) • $Pr[M=m \mid C=c] \overset{\text{BAYES LAW}}{=} Pr[C=c \mid M=m] \cdot \frac{Pr[M=m]}{Pr[C=c]}$

(1) $Pr[C=c] \overset{\text{TOT PROB LAW}}{=}$

↳ C can be generated from all messages. All messages form a partition

PANKO SAYS

$$\sum_{\forall i} Pr[C=c \mid M=m_i] \cdot Pr[M=m_i] =$$

$$= \sum_{\forall i} Pr[K=c \oplus m_i] Pr[M=m_i] = \sum_{\forall i} \frac{1}{2^n} Pr[M=m_i] = \frac{1}{2^n} \sum_{\forall i} Pr[M=m_i] = \frac{1}{2^n}$$

$Pr[K=c \oplus m_i]$: $1/2^n$ (2); $\oplus$: Assumption of OTP

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

So, snap back:

(A) $Pr[M=m \mid C=c] = \frac{Pr[C=c \mid M=m]}{\frac{1}{2^n}} \cdot Pr[M=m]$ (2)

(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

(A) $Pr[M=m \mid C=c] = \frac{1/2^n}{1/2^n} \cdot Pr[M=m] = Pr[M=m]$ So one time pad is perfect.