

Solutions

Cryptography—ENEE/CMSC/MATH 456

Class Exercise 1/29/24

1. Prove or refute: An encryption scheme with message space M is perfectly secret if and only if for every probability distribution over M and every $c_0, c_1 \in C$ we have $\Pr[C = c_0] = \Pr[C = c_1]$. False.

Consider the following slight modification of OTP:

Key Gen: Choose $K \in \mathbb{R} \{0,1\}^L$, choose $b=0$ w/prob $1/4$ and 1 w/prob $3/4$

Enc $_{K||b}$ (m): $m \in \{0,1\}^L$. output ~~output~~ $c||b = m \oplus K || b$.

Dec $_{K||b}$ ($c||b$): output $m := c \oplus K$.

Above is still perfectly secret (show this ~~is~~).

But now, choose any $c \in \{0,1\}^L$ and consider

$$\Pr[C||B = c||0] = \Pr[C=c] \cdot \Pr[B=0] = \Pr[C=c] \cdot 1/4$$

$$\Pr[C||B = c||1] = \Pr[C=c] \cdot \Pr[B=1] = \Pr[C=c] \cdot 3/4$$

2. Prove or refute: An encryption scheme with message space M is perfectly secret if and only if for every probability distribution over M , every $m, m' \in M$ and every $c \in C$ we have $\Pr[M = m | C = c] = \Pr[M = m' | C = c]$. False.

Given any perfectly secret encryption scheme, we choose a distribution over \mathcal{M} and m, m', c s.t.

$$\Pr[M=m | C=c] \neq \Pr[M=m' | C=c]. \text{ This refutes the above.}$$

We choose a distribution over \mathcal{M} that sets

$$\Pr[M=m] > \Pr[M=m'] \text{ for some } m, m'.$$

Now by Def 1 of perfect secrecy $\forall c$:

$$\Pr[M=m | C=c] = \Pr[M=m] \text{ and } \Pr[M=m' | C=c] = \Pr[M=m']$$

$$\text{So } \Pr[M=m | C=c] = \Pr[M=m] > \Pr[M=m'] = \Pr[M=m' | C=c]$$

$$\text{So } \Pr[M=m | C=c] \neq \Pr[M=m' | C=c].$$