# Cryptography: HW1

Trevor Bramwell

Professor Mike Rosulek
January 15, 2015

**1** Perfect secrecy is defined as:

$$\forall m, m' \in M, \text{the distributions } \{k \leftarrow \text{KeyGen}; \text{Enc}(k, m)\}$$
$$\text{and } \{k \leftarrow \text{KeyGen}; \text{Enc}(k, m')\} \text{ are identical.}$$

This means the distribution of possible ciphertexts for any two messages is equal. In other words, they are idependent variables of the ciphertext, and the ciphertext does not depend upon the message.

**a** Let Enc($k$, $m$) $= k \wedge m$, where $\wedge$ is bit-wise AND.

This encryption scheme does not have perfect secrecy. A counterexample is the plaintext bitstrings $m = 10$, and $m' = 11$. These plaintexts have different ciphertext distributions.

$$m = 10, c = \{00, 10\}$$
$$m' = 11, c = \{00, 01, 11\}$$

**b** Let Enc($k$, $m$) $= (k + m) \bmod 2^n$.

$$\begin{aligned} \Pr[c = (k + m) \bmod 2^n] \\ \Pr[(c + 2^n) \bmod 2^n = (k + m) \bmod 2^n] \\ \Pr[(c - m + 2^n) \bmod 2^n = k \bmod 2^n] \\ \Pr[c - m = k \bmod 2^n] \end{aligned}$$

The ciphertext distribution is: $1/(2^n)$

**2** Perfect secrecy states that the distribution of ciphertexts is uniform at random. By Shannon's Theorem this means that for every $m \in M$ and $c \in C$, there exists a unique $k \in K$ such that $\text{Enc}(k, m) = c$. Perfect secrecy states only that $k$ must be unique, not $c$. This means that given two seperate messages $m, m' \in M$, and their cipher texts $c, c' \in C$, for $c = c'$. In english, this means two messages could be encrypted to the same ciphertext. And only given the ciphertext you would not be able to determine, trying every $k \in K$, which plaintext was encrypted.

**3** By reusing the OTP key to encrypt to messages $m$ and $m'$, Alice has leaked $m \oplus m'$ to Eve.

$$\begin{aligned} c &= k \oplus m \\ c' &= k \oplus m' \end{aligned}$$

$$\begin{aligned} c \oplus c' &= k \oplus m \oplus k \oplus m' \\ &= (k \oplus k) \oplus (m \oplus m') \\ &= 0 \oplus (m \oplus m') \\ &= m \oplus m' \end{aligned}$$

Now this may not seem to mean anything. But if for example $m$ and $m'$ were images, this would produce the overlay of both images on top of each other. Quite a leak!

**4** A $t$-out-of-$n$ secret sharing scheme with message space $M$ is secure if, for all deficient sets $X \subseteq \{1, \ldots, n\}$, and $m, m' \in M$, the following distributions are identical:

$$\{S \leftarrow \text{Share}(m); S|_x\} \text{ and } \{S \leftarrow \text{Share}(m'); S|_x\}$$

Given $s_1 < k$ bits long, these distributions would not be equal.

**5** In order for a secreate to be shared between Alice, Bob, Carol, David, Eve, Frank, Gina, Harold, & Irene, the primary secret is first divided into 3 parts in a 3-out-of-3 scheme. Each of these parts is then further divided into a secondary secret in a 2-out-of-3 scheme.

In order for the full secret to be revealed, all 3 parts of the primary secret have to be used, and in order for that to happen, at least 2 out of the 3 members of each subcommittee must be present to reveal the 3 secondary secrets.