# 18-330 Cryptography Notes: Introduction

Note: This is provided as a resource and is not meant to include all material from lectures or recitations. The proofs shown, however, are good models for your homework and exams.

## 1 Symmetric Key Cryptography

**Definition 1.** *A symmetric key cipher consists of 3 polynomial time algorithms:*

1. $KeyGen(\lambda)$*: A randomized algorithm that returns a key* $k \in \mathcal{K}$*.* $\lambda$ *is called the security parameter; typically the strength of* $k$ *should be proportional to* $\lambda$*.*
2. $E(k, m)$*: A potentially randomized algorithm that encrypts a message (or* plaintext*)* $m \in \mathcal{M}$ *with the key* $k$*. It returns a ciphertext* $c$ *in* $\mathcal{C}$*.*
3. $D(k, c)$*: A deterministic algorithm that decrypts* $c$ *with key* $k$*. On success, it returns* $m \in \mathcal{M}$*. Otherwise it fails and returns* $\perp$*.*

We say that the cipher $(KeyGen, E, D)$ is defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$. The textbook definition omits $KeyGen$ in the definition of a Shannon cipher and defines a cipher as $\mathcal{E} = (E, D)$.

## 2 Perfect Secrecy

**Definition 2.** *Let* $\mathcal{M} = \{0, 1\}^n$*. Consider an experiment where the random variable* $k$ *is uniformly distributed over* $\mathcal{K}$*. An encryption scheme is perfectly secure if:*

$$\forall m_0, m_1 \in M, \forall c \in C, Pr[E(k, m_0) = c] = Pr[E(k, m_1) = c]$$

*where the probability is over the choice of* $k$*.*

### 2.1 Shannon's Theorem

**Theorem 1.** *Let* $\mathcal{E} = (KeyGen, E, D)$ *be a Shannon cipher defined over* $(\mathcal{K}, \mathcal{M}, \mathcal{C})$*. If* $\mathcal{E}$ *is perfectly secure, then* $|\mathcal{K}| \geq |\mathcal{M}|$*.*

### 2.2 One Time Pad: Proof of Perfect Secrecy

**Definition 3.** *One Time Pad (OTP) is an encryption scheme. We define it as follows over* $\mathcal{M} = \mathcal{C} = \mathcal{K} = \{0, 1\}^\lambda$*:*

- $KeyGen(\lambda)$*: Choose* $k$ *uniformly at random from* $\mathcal{K}$*.*

- $E(k, m) = k \oplus m = c$
- $D(k, c) = k \oplus c = m$

We prove that this scheme is perfectly secure:

*Proof.* Suppose that $\mathcal{E} = (KeyGen, E, D)$ is a one-time pad defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{K} := \mathcal{M} := \mathcal{C} := \{0,1\}^\lambda$. Consider any messages $m_1, m_2 \in \mathcal{M}$ and ciphertext $c \in \mathcal{C}$. Notice that for any key $m \in \mathcal{M}$, there exists only one $k$ such that $m \oplus k = c$. Why? Suppose there were two different keys $k_0, k_1 \in \mathcal{K}$ where $k_0 \neq k_1$, but $m \oplus k_0 = c = m \oplus k_1$. Then if we XOR both sides with $m$, we get:

$$\begin{aligned} m \oplus m \oplus k_0 &= m \oplus m \oplus k_1 \\ 0 \oplus k_0 &= 0 \oplus k_1 \\ k_0 &= k_1 \end{aligned}$$

but we started from the assumption that $k_0 \neq k_1$, which means we arrived at a contradiction. Hence, only one $k$ can satisfy $m \oplus k = c$.
Hence, in our main proof, we have:

$$\begin{aligned} Pr[E(m_1) = c] &= \frac{\left|\{k \in \{0,1\}^\lambda : k \oplus m_1 = c\}\right|}{|\mathcal{K}|} \\ &= \frac{1}{2^\lambda} \end{aligned}$$

Nothing about the calculations above made use of any specific information about $m_1$, so we by the same logic, we can conclude that $Pr[E(m_2) = c] = \frac{1}{2^\lambda}$. We conclude that for any $m_1, m_2, c$, $Pr[E(k, m_1) = c] = Pr[E(k, m_2) = c]$ holds, and therefore $\mathcal{E}$ is perfectly secure. □

# 3 Miscellaneous

This class doesn't distinguish between polynomial time (PT) algorithms and probabilistic polynomial time (PPT) algorithms. A PPT algorithm is different from a PT algorithm in that it runs in polynomial time *in expectation*. This isn't important for class, but occasionally PPT is mentioned in place of PT and vice versa.