SAPIENZA
UNIVERSITÀ DI ROMA

"Sapienza" University of Rome
Faculty of Information Engineering, Informatics and Statistics
Department of Computer Science

Cryptography

Lecture notes integrated with the book "Introduction to Modern Cryptography", J. Katz, Y. Lindell

Author
Simone Bianco

September 30, 2025

Contents

Information and Contacts

Personal notes and summaries collected as part of the *Cryptography* course offered by the degree in Computer Science of the University of Rome "La Sapienza".

Further information and notes can be found at the following link:
https://github.com/Exyss/university-notes. Anyone can feel free to report inaccuracies, improvements or requests through the Issue system provided by GitHub itself or by contacting the author privately:

- Email: **bianco.simone@outlook.it**
- LinkedIn: **Simone Bianco**

The notes are constantly being updated, so please check if the changes have already been made in the most recent version.

Suggested prerequisites:

Algebra and Computational Complexity

Licence:

1

Introduction to modern cryptography

1.1 Definitions, assumptions and notation

Cryptography is the branch of computer science that practices and studies techniques for secure communication in the presence of adversarial behavior (e.g. altering the integrity of the message, reading the content of the message, ...). Cryptography focuses on two main goals:

1. **Confidential communication**: the property of making the original message impossible to read even if an outsider finds out the *cyphertext*, i.e. the encrypted message

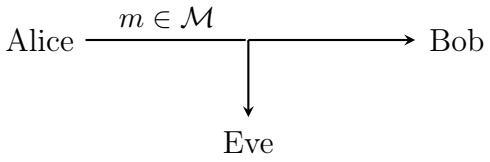

Figure 1.1: Without an encryption scheme, Eve – an evildoer – may be able to read the message that Alice is sending to Bob.

2. **Message integrity**: the capability of ensuring that the original message has not been altered even if an outsider intercepts the cyphertext

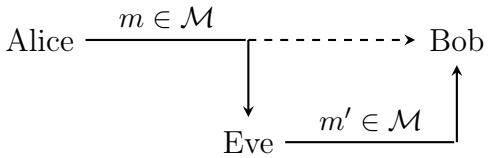

Figure 1.2: Without an encryption scheme, Eve may be able to intercept and alter the message that Alice is sending to Bob.

Before the 50's, cryptography was considered an *art* for geniouses capable of encrypting and decrypting messages written by other geniouses of the field. In modern days, cryptography became a *mathematical science* with precise definitions and proofs. These mathematical tools separate in two types: **unconditional proofs** and **conditional proofs**.

The former type referres to proofs where no assumptions are made, focusing on showing that something is possible without caring about it being inefficient (hence we have theoretically infinite resources at our disposal). The latter, instead, uses real-world assumptions that are believed to be true in order to prove real-world results. The typical example is the $\mathsf{P} \neq \mathsf{NP}$ assumption, i.e. that there are some problems that are verifiable in polynomial time but not solvable in polynomial time. Many cryptosystems are based on the assumption that prime factorization is hard to solve but easy to verify. This is equivalent to assuming that FACTORING $\in \mathsf{NP} - \mathsf{P}$ (only FACTORING $\in \mathsf{NP}$ has been proven), making the assumption $\mathsf{P} \neq \mathsf{NP}$ fundamental. Making a crytosystem easy to verify allows us to make it impossible to access a resource without using knowing the solution to the authentication phase.

Theorem 1.1

Every cryptosystem based on prime factorization is "secure" if FACTORING $\notin \mathsf{P}$

Proof (sketch). By contrapositive, suppose that there is a cryptosystem Π that is not "secure", meaning that there is a polynomial time algorithm A that is capable of "breaking" Π. Then, for each number $n \in \mathbb{N}$ we can forge a message m based on n and use the output $A(m)$ to find the prime factors of n, concluding that $\mathsf{FACTORING} \in \mathsf{P}$. □

These two goals will be discussed under two main types of cryptosystems:

- **Symmetric cryptography**: both ends of the communication share a single common key that is random and unknown to any outsider.
- **Asymmetric cryptography**: both ends of the communication have each their own key pair (pk, sk) where pk is *public*, i.e. known by everyone, and sk is *secret*, i.e. known only by the owner.

Throughout this work we'll use the following notation to talk about cryptographic systems:

- $\mathcal{M}$ is the message space, i.e. the set of all strings of messages that can be sent between two parties.
- $\mathcal{C}$ is the cyphertext space, i.e. the set of all strings of cyphertexts that can be produced by a cryptosystem.
- $\mathcal{K}$ is the key space, i.e. the set of all strings of keys that can be used in a cryptographic system.
- $\mathcal{H}$ is the hashing function space, i.e. the set of all hash functions that can be used by a cryptosystem.

2

Information-theoretic cryptography

2.1 Perfect secrecy and Shannon's theorem

For now, we'll focus on symmetric cryptography, i.e. cryptosystems where a shared secret key is used for both encryption and decryption. It is widely used due to its speed and efficiency, especially in encrypting large volumes of data. A core model of this approach is **Secret Key Encryption (SKE)**, which includes three main components:

- A shared *secret key* $K \in_R \mathcal{K}$ chosen uniformly at random
- An *encryption function* $\text{Enc} : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ that transforms plaintext into cyphertext
- A *decryption function* $\text{Dec} : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$ that transforms a cyphertext into plaintext

In order to be functional, SKEs must be **correct**, meaning that if a message $m \in \mathcal{M}$ gets encrypted with $K \in_R \mathcal{K}$ obtaining the cyphertext $c \in \mathcal{C}$, the decryption process over c using the same key K must give back the original message.

Definition 2.1: Correctness in SKEs

An SKE $\Pi = (\text{Enc}, \text{Dec})$ is said to be correct if $\forall m \in \mathcal{M}, \forall K \in_R \mathcal{K}$ it holds that:

$$\text{Dec}(K, \text{Enc}(K, m)) = m$$

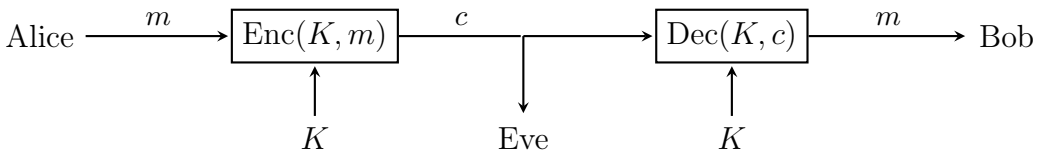

Figure 2.1: Example of SKE with perfect secrecy. Even if Eve intercepts the cyphertext, she cannot obtain the original message since she doesn't know the key.

Originally proposed in the 19th century by the homonym cryptographer, **Kerckhoffs's principle** is a foundational concept in cryptography which asserts that the security of a cryptographic system should depend only on the secrecy of the key. In other words, a system should be secure even if everything about the system is known publicly, except for the secret key. The principle was later succinctly restated by Claude Shannon as "the enemy knows the system".

During his work, Shannon also proposed a formal definition of **perfect secrecy**, i.e. a property that fully respects the concept behind Kerckhoff's principle. Shannon's formulation states that the probability of m being the communicated message is equal to the probability of m being the communicated message even when the corresponding cyphertext c is known. In other words, no cyphertext reveals additional information over any message.

Definition 2.2: Perfect secrecy

Let $\Pi = (\text{Enc}, \text{Dec})$ be an SKE. Let M be a random variable over $\mathcal{M}$ and let C be another random variable defined as $C = \text{Enc}(K, M)$, for some key $K \in_R \mathcal{K}$. We say that Π has perfect secrecy when $\forall m \in \mathcal{M}$ and $\forall c \in \mathcal{C}$ it holds that:

$$\Pr[M = m] = \Pr[M = m \mid C = c]$$

Shannon proved that such definition is achievable by some cryptosystems, but it comes with inheritent practical limitations. Suprisingly, even a simple SKE as the **One Time Pad (OTP)** system has perfect secrecy. In this system we assume that everything is a binary string of the same length, i.e. that $\mathcal{M} = \mathcal{K} = \mathcal{C} = \{0,1\}^n$ for some $n \in \mathbb{N}$. The encryption and decryption functions are defined as follows:

$$\text{Enc}(K, m) = K \oplus m \qquad \text{Dec}(K, c) = K \oplus c$$

By properties of the bit-wise XOR function, it's easy to see that OTP is complete:

$$\text{Dec}(K, \text{Enc}(K, m)) = K \oplus (K \oplus m) = m$$

In order to prove that OTP has perfect secrecy, we start by proving two equivalent definitions of perfect secrecy. In particular, states that for every pair of messages every cyphertext has the same probability of being the output of the encoding function when applied of both messages.

Lemma 2.1: Perfect secrecy (eq. definitions)

Let $\Pi = (\text{Enc}, \text{Dec})$ be an SKE. Let M be a random variable over $\mathcal{M}$ and let C be another random variable defined as $C = \text{Enc}(K, M)$, for some key $K \in_R \mathcal{K}$. The following statements are equivalent:

1. Π has perfect secrecy
2. M and C are independent
3. $\forall m, m' \in \mathcal{M}$ and $\forall c \in \mathcal{C}$ it holds that:

$$\Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m) = c] = \Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m') = c]$$

Proof. $\Longrightarrow$ 2. Suppose that Π has perfect secrecy. Then, through definition of conditional probability we get that:

$$\Pr[M = m] = \Pr[M = m \mid C = c] = \frac{\Pr[M = m, C = c]}{\Pr[C = c]}$$

which implies that:

$$\Pr[M = m] \cdot \Pr[C = c] = \Pr[M = m, C = c]$$

concluding that M and C are independent

1. Suppose that M and C are independent. Fix $m, m' \in \mathcal{M}$ and $c \in \mathcal{C}$. Through event manipulation and independency of M and C we obtain that:

$$\begin{aligned}\Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m) = c] &= \Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, M) = c \mid M = m] \\ &= \Pr_{K \in_R \mathcal{K}}[C = c \mid M = m] \\ &= \Pr_{K \in_R \mathcal{K}}[M = m]\end{aligned}$$

Since every message has the same probability of being correct – without additional information – we know that:

$$Pr_{K \in_R \mathcal{K}}[M = m] = Pr_{K \in_R \mathcal{K}}[M = m']$$

Moreover, through a similar argument to the one above we get that:

$$\Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m') = c] = \Pr_{K \in_R \mathcal{K}}[M = m']$$

2. Assume the third statement holds and fix $c \in \mathcal{C}$

Claim: $\Pr[C = c] = \Pr[C = c \mid M = m]$

Proof of the claim. Through the probability sum principle, we get that:

$$\begin{aligned}\Pr[C=c] &= \sum_{m'\in\mathcal{M}} \Pr[C=c, M=m] \\ &= \sum_{m'\in\mathcal{M}} \Pr[C=c \mid M=m'] \cdot \Pr[M=m'] \\ &= \sum_{m'\in\mathcal{M}} \Pr[\mathrm{Enc}(K,M')=c \mid M=m'] \cdot \Pr[M=m'] \\ &= \sum_{m'\in\mathcal{M}} \Pr[\mathrm{Enc}(K,m')=c] \cdot \Pr[M=m']\end{aligned}$$

Through the hypothesis we also get that:

$$\begin{aligned}\Pr[C=c] &= \sum_{m'\in\mathcal{M}} \Pr[\mathrm{Enc}(K,m')=c] \cdot \Pr[M=m'] \\ &= \sum_{m'\in\mathcal{M}} \Pr[\mathrm{Enc}(K,m)=c] \cdot \Pr[M=m'] \\ &= \Pr[\mathrm{Enc}(K,m)=c] \cdot \sum_{m'\in\mathcal{M}} \Pr[M=m'] \\ &= \Pr[\mathrm{Enc}(K,m)=c] \cdot 1 \\ &= \Pr[\mathrm{Enc}(K,M)=c \mid M=m] \\ &= \Pr[C=c \mid M=m]\end{aligned}$$

□

By definition of conditional probability, we know that:

$$\Pr[M=m \mid C=c]\cdot\Pr[C=c] = \Pr[M=m, C=c] = \Pr[C=c \mid M=m]\cdot\Pr[M=m]$$

which implies that:

$$\Pr[M=m] = \frac{\Pr[M=m \mid C=c] \cdot \Pr[C=c]}{\Pr[C=c \mid M=m]}$$

Finally, through the claim we conclude that:

$$\Pr[M=m] = \frac{\Pr[M=m \mid C=c] \cdot \Pr[C=c]}{\Pr[C=c \mid M=m]} = \Pr[M=m \mid C=c]$$

□

Theorem 2.1

OTP has perfect security.

Proof. We'll prove that the third definition of Lemma 2.1 holds for OTP. Fix two messages $m, m' \in \mathcal{M}$ and a cyphertext $c \in \mathcal{C}$. Through definition of the OTP system and by the properties of the XOR function, we have that:

$$\Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m) = c] = \Pr_{K \in_R \mathcal{K}}[K \oplus m = c] = \Pr_{K \in_R \mathcal{K}}[K = m \oplus c] = 2^{-n}$$

Through the same argument, we also get that:

$$\Pr_{K \in_R \mathcal{K}}[\text{Enc}(K, m') = c] = 2^{-n}$$

□

We'll now show the inheritent limitations of perfect secrecy. The key idea is simple: in order for M and C to be independent, the key cannot be shorter than the message. Otherwise, there will be some cyphertexts that are unreachable by some messages, revealing information on the system.

Theorem 2.2: Shannon's perfect secrecy theorem

Let $\Pi = (\text{Enc}, \text{Dec})$ be a non-trivial perfectly secret SKE. Then, it holds that $|\mathcal{K}| \geq |\mathcal{M}|$

Proof. Suppose that Π is a non-trivial perfectly secret. Fix any $c \in \mathcal{C}$ such that $\Pr[C = c] > 0$ (this is where non-triviality is required). Let $\mathcal{M}'$ be the set of possible decryptions over c, i.e. $\mathcal{M}' = \{\text{Dec}(K, c) \mid K \in \mathcal{K}\}$. We observe that $\mathcal{M}'$ contains at most one decryption for each key (some keys may yield the same decryption). By way of contradiction, suppose that $|\mathcal{K}| < |\mathcal{M}|$. Then, we get that $|\mathcal{M}'| \leq |\mathcal{K}| < |\mathcal{M}|$.

This implies that $\exists m \in \mathcal{M} - \mathcal{M}'$. Thus, there is a message that cannot be the result of applying the decryption function on c, meaning that $\Pr[M = m \mid C = c] = 0$. However, we know that, when no additional information is given, every message is uniform, hence $\Pr[M = m] = \frac{1}{\mathcal{M}}$, contradicting the fact that Π has perfect secrecy. □

2.2 Message Authentication Codes (MACs)

We'll now focus on the second key goal of cryptography: *message integrity*. The simplest way to reach such goal is through **Message Authentication Codes (MACs)**, an additional piece of information sent with the message that enables the receiver to assert that the message hasn't been altered.

For now, we'll start with a simple model that doesn't care about secrecy, but only about integrity. This type of MACs use a deterministic **tagging function** (usually implemented as an *hash function*) $\text{Tag} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}$, where $\mathcal{T}$ is the tag space, i.e. the set of all tag strings.

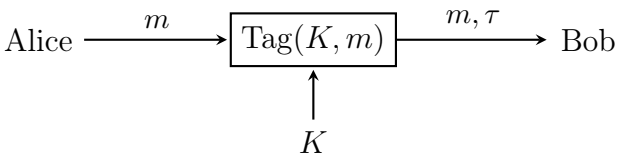

Figure 2.2: Example of an integrity-only MAC.

The idea behind tagging functions is simple: once the message and the tag have been received, Bob can re-compute the tag using the same key-message pair and compare it to the received tag. If the two tags are equal, Bob is sure that the message hasn't been altered. However, this simple idea can only work under the assumption of **unforgeability**:

- It should be hard to forge a valid tag τ for a message m when the key K is not known
- It should be hard to forge a valid tag τ for a message m even when a pair (m', τ') is known

In other words, unforgeability states that no pair should reveal no information about how the tags are computed. Without this property, an adversarial entity may be able to infer information on the shared key and/or the tagging function, using them to forge valid tags. If an entity is capable of forging a valid tag, it may intercept the message-tag pair, alter the message, forge a valid tag for the new message and send a new pair, fooling the receiver. We give a formal definition of a property that reflects this unforgeability aspect.

Definition 2.3: t-time ε-statistical security

We say that a MAC $\Pi = (\text{Tag})$ has t-time ε-statistical security when $\forall m, m_1, \ldots, m_t \in \mathcal{M}$ with $m \neq m'$ and $\forall \tau, \tau_1, \ldots, \tau_t \in \mathcal{T}$ it holds that:

$$\Pr_{K \in_R \mathcal{K}}[\text{Tag}(K, m) = \tau \mid \text{Tag}(K, m_1) = \tau_1, \ldots, \text{Tag}(K, m_t) = \tau_t] \leq \varepsilon$$

In simple terms, the above property states that, even when t message-tag pairs $(m_1, \tau_1), \ldots, (m_t, \tau_t)$ are known, the probability of a message-tag pair (m, τ) being possible is at most ε. Optimally, we want ε to be as small as possible and t to be as large as possible. However, it's easy to see that $\forall t \in \mathbb{N}$ it is impossible to get $\varepsilon = 0$ since a random $\tau \in \mathcal{T}$ always has probability at least $\frac{1}{|\mathcal{T}|}$ of being correct. Just as we did with perfect secrecy, we'll show that the notion of good statistical security is achievable, but it's highly inefficient in terms of key size.

Theorem 2.3

Any t-time $2^{-\lambda}$-statistically secure MAC must have a key of size $(t+1)\lambda$

Proof. Omitted. □

A good enough 1-time statistically secure MAC is achievable through **pairwise independent hash functions**, i.e. a family of hash functions where each pair of functions forms a pair of independent random variables. This idea can also be expressed through joint uniform distributions, as in the below definition.

Definition 2.4: Pairwise independent hash functions

Let $\mathcal{H} = \{h_K : \mathcal{M} \to \mathcal{T}\}_{K \in \mathcal{K}}$ be a family of hash functions. We say that $\mathcal{H}$ is pairwise independent if $\forall m, m' \in \mathcal{M}$ with $m \neq m'$ it holds that the distribution $(h_K(m), h_K(m'))$ is uniform over $\mathcal{T} \times \mathcal{T}$ when $K \in_R \mathcal{K}$.

Note: $h_K(m)$ and $h_K(m')$ denote two random variables in this context.

Theorem 2.4

Let $\mathcal{H} = \{h_K : \mathcal{M} \to \mathcal{T}\}_{K \in \mathcal{K}}$ be a family of pairwise indepependent hash functions induces a 1-time $\frac{1}{|\mathcal{T}|}$-statistically secure MAC.

Proof. Fix $m \in \mathcal{M}$ and $\tau \in \mathcal{T}$. Let $\Pi = (\text{Tag})$ be the MAC defined as $\text{Tag}(K, m) = h_K(m)$. Since the joint probability of each pair of hash functions in $\mathcal{H}$ is pairwise uniformly distributed, we get that each hash function is also individually uniformly distributed. Hence, we derive that:

$$\Pr[\text{Tag}(K, m) = \tau] = \Pr[h_K(m) = \tau] = \frac{1}{|\mathcal{T}|}$$

Similarly, by pairwise independence $\forall m, m' \in \mathcal{M}$ with $m \neq m'$ and $\forall \tau, \tau' \in \mathcal{T}$ it holds that:

$$\begin{aligned}
\Pr_{K \in_R \mathcal{K}}[\text{Tag}(K, m') = \tau', \text{Tag}(K, m) = \tau] &= \Pr_{K \in_R \mathcal{K}}[\text{Tag}(K, m') = \tau'] \cdot \Pr_{K \in_R \mathcal{K}}[\text{Tag}(K, m') = \tau'] \\
&= \Pr_{K \in_R \mathcal{K}}[h_K(m') = \tau'] \cdot \Pr_{K \in_R \mathcal{K}}[h_K(m) = \tau] \\
&= \frac{1}{|\mathcal{T}|} \cdot \frac{1}{|\mathcal{T}|}
\end{aligned}$$

Putting the two results together we get that:

$$\Pr[\text{Tag}(K, m') = \tau' \mid \text{Tag}(K, m) = \tau] = \frac{\Pr_{K \in_R \mathcal{K}}[\text{Tag}(K, m') = \tau', \text{Tag}(K, m) = \tau]}{\Pr[\text{Tag}(K, m) = \tau]} = \frac{1}{|\mathcal{T}|}$$

□

After proving that pairwise independent hash function families form a good enough MAC, we're left with proving that such families exist. Suprisingly, these families can be easily constructed through prime numbers.

Proposition 2.1

Given a prime $p \in \mathbb{P}$, let $\mathcal{M} = \mathcal{T} = \mathbb{Z}_p$ and $\mathcal{K} = \mathbb{Z}_p^2$. Then, the family $\mathcal{H} = \{h_{(a,b)}\}_{(a,b)\in\mathbb{Z}_p^2}$ where $h_{(a,b)}(m) = am + b \pmod p$ is pairwise independent.

Proof. Fix $m, m' \in \mathbb{Z}_p$ with $m \neq m'$ and $\tau, \tau' \in \mathbb{Z}_p$. We'll show that the joint probability over the hash functions is uniform. First, we observe that:

$$\begin{aligned}\Pr_{(a,b)\in_R\mathbb{Z}_p^2}[h_{(a,b)}(m) = \tau, h_{(a,b)}(m') = \tau'] &= \Pr_{(a,b)\in_R\mathbb{Z}_p^2}[am + b = \tau, am' + b = \tau'] \\ &= \Pr_{(a,b)\in_R\mathbb{Z}_p^2}\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau \\ \tau' \end{pmatrix}\right]\end{aligned}$$

Since $m \neq m'$, we know that $\det(\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}) = m - m' \neq 0$, thus the matrix is invertible. This allows us to further manipulate the event and rewrite it in terms of the key:

$$\begin{aligned}\Pr_{(a,b)\in_R\mathbb{Z}_p^2}[h_{(a,b)}(m) = \tau, h_{(a,b)}(m') = \tau'] &= \Pr_{(a,b)\in_R\mathbb{Z}_p^2}\left[\begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} \tau \\ \tau' \end{pmatrix}\right] \\ &= \Pr_{(a,b)\in_R\mathbb{Z}_p^2}\left[\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} m & 1 \\ m' & 1 \end{pmatrix}^{-1}\begin{pmatrix} \tau \\ \tau' \end{pmatrix}\right] \\ &= \frac{1}{|\mathbb{Z}_p^2|}\end{aligned}$$

concluding that $\mathcal{H}$ is pairwise independent. □

2.3 Randomness extraction

We discussed how randomness can be used to generate secret keys over a probability distribution, but how a random value be generated? As we will discuss later, randomness is a crucial concept for secure cryptography. Clearly, there is no such concept as *real randomness*: even if the whole universe may appear chaotic, everything is technically deterministic. The process of generating a random-enough value is called **randomness extraction** and it is typically achieved by measuring physical quantities (noise, air humidity, ...) in order to produce a short unpredictable sequence of bits (e.g. 256 bits), which is expensive to generate and not necessarily uniform. This short "truly random" sequence gets usually expanded to any desired length – as long as it is polynomial with respect to the original lenght – through the use of a **pseudo-random generator (PRG)**. However, this process requires some strict computational assumptions, which we'll discuss later.

For now, we'll focus on understanding how to extract randomness from an unpredictable secure variable X. The first **extractor** that sparked the idea is Von Neumann's Extractor, which yields a fair random coin from an unpredictable unfair one. Let $B \in \{0, 1\}$ be the

random variable describing the unpredictable unfair coin, where $\Pr[B = 0] = p < \frac{1}{2}$. Let $Y \in \{0, 1\}$ be the random variable describing our new coin. The value of Y is determined by the following procedure. Sample two values b_1, b_2 from B at different times. If $b_1 = b_2$, Y assumes no value (marked as $Y =?$) and we repeat the sampling process. If not, $Y = 1$ if $b_1 = 0$ and $b_2 = 1$, otherwise $Y = 0$ if $b_1 = 1$ and $b_2 = 0$.

If the sampling process succeeds, i.e. Y assumes a value, we have that $\Pr[Y = 0] = p(1-p)$ and $\Pr[Y = 1] = (1 - p)p$, thus $\Pr[Y = 0] = \Pr[Y = 1]$. Moreover, we observe that the probability of $Y == ?$ being true for m consecutive tries is at most:

$$\Pr[Y =? \text{ for } m \text{ tries}] = (\Pr[Y == ?])^m = (1 - \Pr[Y = 0 \cup Y = 1])^m \leq (1 - 2p(1 - p))^m$$

As m grows to infinity, the latter probability goes to 0, making the even negligible. Implying that $\Pr[Y = 0]$ and $\Pr[Y = 1]$ tend to be $\frac{1}{2}$ due to them having the same probability and them being the only two outcomes. This makes Y a fair enough coin.

Our goal is to generalize this concept to any desider value, i.e. design an extractor Ext that uses a random variable X to output any desided uniform distribution $\text{Ext}(X)$. A good eye may recognize that this is clearly impossible to achieve unless the source is already truly unpredictable, which makes the extractor useless since we already have a truly random source. As for many computational and probabilistic concepts, we can only hope to achieve something that is good-enough for our purposes. This goodness is measured through a concept known as **min-entropy**, that being the largest value m having the property that each observation of X provides at least m bits of information.

Definition 2.5: Min-entropy

Given a random variable X, we define the min-entropy of X as:

$$H_{\min}(X) = -\log \max_x \Pr[X = x]$$

One way to justify the name of the quantity is to compare it with the more standard definition of *entropy*, defined as the expectation value of $\log\left(\frac{1}{p_i}\right)$ over a distribution P

$$H(P) = \sum_i p_i \log\left(\frac{1}{p_i}\right)$$

In the min-entropy, instead, we take take the minimum value of $\log\left(\frac{1}{p_i}\right)$, where:

$$\min_i \log\left(\frac{1}{p_i}\right) = \log\left(\min_i \frac{1}{p_i}\right) = -\log \max_i p_i$$

Consider a random variable $X \sim U_n$, where U_n is an uniform distribution over $\{0, 1\}^n$. In this case, we have that $\Pr[X = x] = 2^{-n}$ for all value x assumable by X. Hence, the min-entropy is:

$$H_{\min}(X) = -\log \max_x \Pr[X = x] = -\log(2^{-n}) = n$$

This concludes that each observation of X provides at least n bits of information. Consider now a constant random variable X', i.e. $\Pr[X' = x^*] = 1$ for some fixed value x^* and $\Pr[X' = x] = 0$ for every $x^* \neq x$. It's easy to see that:

$$H_{\min}(X') = -\log \max_{x'} \Pr[X' = x] = -\log 1 = 0$$

Concluding that each observation of X' provides at least 0 bits of information. This information-theoretic measure opens a new question regarding extractors: is there an extractor Ext^* that for any random variable X outputs an uniform distribution $Y = \text{Ext}(X)$ such that $H_{\min}(X) \geq k$ for some value $k > 0$? Even under these constraints, the answer to this question is still negative. In particular, it's impossible to define such extractor even if we restrict our interest to extracting only one bit while revealing at least one bit less than the input length.

Proposition 2.2

Let X be a random variable defined over $\{0,1\}^n$. There is no extractor Ext such that $\text{Ext}(X) \in \{0,1\}$.

Proof. Let $\text{Ext} : \{0,1\}^n \to \{0,1\}$ be any extractor and let $b \in \{0,1\}$ be the output minimizing the cardinality of the preimage of the extractor, i.e. the set of inputs for which the extractor outputs b.

$$b = \arg\min_{b' \in \{0,1\}} \left|\text{Ext}^{-1}(b)\right|$$

By the pidgeonhole principle, we have that $\left|\text{Ext}^{-1}(b)\right| \geq \frac{|\{0,1\}^n|}{2} = 2^{n-1}$. Let X be a random variable uniform over $\text{Ext}^{-1}(b)$. Since X is uniform, we have that $H_{\min}(X) \geq n-1$. However, we know that $\text{Ext}(X)$ isn't uniform due to the output being always b. This concludes that any extractor has always a bad input uniform random variable X that returns a non-uniform distribution $\text{Ext}(X)$. □

Since we can't define an extractor that yields an uniform distribution, the best we can hope for is a distribution that is close enough to an uniform one. We use a standard measure for distribution similarity, called **ε-closeness**.

Definition 2.6: ε-closeness

Let X, X' be two random variables defined over the same set. We say that X and X' are ε-close, written as $X \sim_\varepsilon X'$ when their *statistical distance* $\text{SD}(X; X')$ is at most ε, where:

$$\text{SD}(X; X') = \frac{1}{2} \sum_x |\Pr[X = x] - \Pr[X' = x]|$$

The concept of ε-closeness between two random variables is equivalent to saying that every *unbounded adversary* A, i.e. an entity with unlimited computational power that

wants to break our system, cannot distinguish whether a value x has been sampled from X or X'.

$$|\Pr[A(x) = 1 : x \leftarrow X] - \Pr[A(x) = 1 : x \leftarrow X']| \leq \varepsilon$$

Definition 2.7: Deterministic extractor

Let S be a random variable, referred to as *seed*. We say that $\text{Ext} : \{0,1\}^d \times \{0,1\}^n \to \{0,1\}^\ell$ is a (k, ε)-extractor if for every random variable X with $H_{\min}(X) \geq k$ it holds that $(S, \text{Ext}(S, X)) \sim_\varepsilon (S, U_\ell)$ when $S \sim U_d$.

We notice that the condition $(S, \text{Ext}(S, X)) \sim_\varepsilon (S, U_\ell)$ implies that the seed must be *public*. This requirement is forced in order to avoid trivial extractors such as $\text{Ext}(S, X) = S$.

Proposition 2.3

Let Y be a random variable over a set $\mathcal{Y}$ and assume that its *collision probability* is:

$$\text{Col}(Y) = \sum_y \Pr[Y = y]^2 \leq \frac{1}{|\mathcal{Y}|}(1 + 4\varepsilon^2)$$

Then, it holds that $\text{SD}(Y, U) \leq \varepsilon$.

Proof. TODO. □

Lemma 2.2: Left-over hash lemma

Let $\mathcal{H} = \{h_S : \{0,1\}^n \to \{0,1\}^\ell\}_{S \in \{0,1\}^d}$ be a pairwise independent hash function. Then, $\text{Ext}(S, X) = h_S(x)$ is a (k, ε)-extractor for $k \geq \ell + 2\log\left(\frac{1}{\varepsilon}\right) - 2$

Proof. TODO. □

2.4 Solved exercises

Problem 2.1

Given a prime $p \in \mathbb{P}$, let $\mathcal{M} = \mathcal{T} = \mathbb{Z}_p$ and $\mathcal{K} = \mathbb{Z}_p^2$. Prove that the hash family $\mathcal{H} = \{h_{(a,b)}\}_{(a,b) \in \mathbb{Z}_p^2}$, where $h_{(a,b)}(m) = am + b \pmod p$, cannot be a 2-time statistically secure MAC

Problem 2.2

Construct a 3-wise independent hash function family and prove it's correctness.