# Cryptography—Homework 1*

Sapienza University of Rome
Master's Degree in Computer Science
Master's Degree in Cybersecurity
Master's Degree in Mathematics

Daniele Venturi

*Due Date: November 17, 2020 (23:59 CET)*

## 1 Perfect Secrecy 20 Points

(a) Prove or refute: An encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ with key space $\mathcal{K}$, message space $\mathcal{M}$, and ciphertext space $\mathcal{C}$ is perfectly secret if and only if the following holds: For every probability distribution $M$ over $\mathcal{M}$, and every $c_0, c_1 \in \mathcal{C}$, we have $\Pr[C = c_0] = \Pr[C = c_1]$, where $C := \mathsf{Enc}(K, M)$ with $K$ uniform over $\mathcal{K}$.

(b) For each of the following encryption schemes, state whether the scheme is perfectly secret. Justify your answer in each case.

(i) The message space is $\mathcal{M} = \{0, \ldots, 4\}$. The secret key is uniform over the key space $\mathcal{K} = \{0, \ldots, 5\}$. The encryption algorithm $\mathsf{Enc}(k, m)$ returns $c = k + m \bmod 5$, whereas the decryption algorithm $\mathsf{Dec}(k, c)$ returns $c - k \bmod 5$.

(ii) The message space is $\mathcal{M} = \{m \in \{0,1\}^\ell : \text{the last bit of } m \text{ is } 0\}$. The secret key is uniform over the key space $\mathcal{K} = \{0,1\}^{\ell-1}$. The encryption algorithm $\mathsf{Enc}(k, m)$ returns $c = m \oplus (k||0)$, whereas the decryption algorithm $\mathsf{Dec}(k, c)$ returns $c \oplus (k||0)$.

## 2 Universal Hashing 20 Points

(a) A family $\mathcal{H} = \{h_s : \mathcal{X} \to \mathcal{Y}\}_{s \in \mathcal{S}}$ of hash functions is called $t$-wise independent if for all sequences of *distinct* inputs $x_1, \ldots, x_t \in \mathcal{X}$, and for any output sequence

*Some of the exercises are taken from the book *"Introduction to Modern Cryptography"* (second edition), by Jonathan Katz and Yehuda Lindell.

$y_1, \ldots, y_t \in \mathcal{Y}$ (not necessarily distinct), we have that:

$$\Pr\left[h_s(x_1) = y_1 \wedge \cdots \wedge h_s(x_t) = y_t : \; s \leftarrow_{\$} \mathcal{S}\right] = \frac{1}{|\mathcal{Y}|^t}.$$

(i) For any $t \geq 2$, show that if $\mathcal{H}$ is $t$-wise independent, then it is also $(t-1)$-wise independent.

(ii) Let $q$ be a prime. Show that the family $\mathcal{H} = \{h_s : \mathbb{Z}_q \to \mathbb{Z}_q\}_{s \in \mathbb{Z}_q^3}$, defined by

$$h_s(x) := h_{s_0,s_1,s_2}(x) := s_0 + s_1 \cdot x + s_2 \cdot x^2 \bmod q$$

is 3-wise independent.

(b) Say that $X$ is a $(k, n)$-source if $X \in \{0,1\}^n$, and the min-entropy of $X$ is at least $k$. Answer the following questions:

(i) Suppose that $\ell = 128$; what is the minimal amount of min-entropy needed in order to obtain statistical error $\varepsilon = 2^{-80}$ when applying the leftover hash lemma? What is the entropy loss?

(ii) Suppose that $k = 238$; what is the maximal amount of uniform randomness that you can obtain with statistical error $\varepsilon = 2^{-80}$ when applying the leftover hash lemma? Explain how to obtain $\ell = 320$ using computational assumptions.

## 3 One-Way Functions 20 Points

(a) Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a PRG with $\lambda$-bit stretch. Prove that $G$ is by itself a one-way function.

(b) Let $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$ be a PRG with one-bit stretch. Prove that $G$ is by itself a one-way function.

## 4 Pseudorandom Generators 20 Points

(a) Let $G_1, G_2 : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be two deterministic functions mapping $\lambda$ bits into $\lambda + \ell$ bits (for $\ell \geq 1$). You know that at least one of $G_1$, $G_2$ is a secure PRG, but you don't know which one. Show how to design a secure PRG $G^* : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda+\ell}$ by combining $G_1$ and $G_2$.

(b) Can you prove that your construction works when using the same seed $s^* \in \{0,1\}^\lambda$ for both $G_1$ and $G_2$? Motivate your answer.

## 5 Pseudorandom Functions — 25 Points

(a) Show that no PRF family can be secure against computationally unbounded distinguishers.

(b) Analyze the following candidate PRFs. For each of them, specify whether you think the derived construction is secure or not; in the first case prove your answer, in the second case exhibit a concrete counterexample.

(i) $F_k(x) = G'(k) \oplus x$, where $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ is a PRG, and $G'$ denotes the output of $G$ truncated to $\lambda$ bits.

(ii) $F_k(x) := F_x(k)$, where $F : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\ell$ is a PRF.

(iii) $F'_k(x) = F_k(x||0)||F_k(x||1)$, where $x \in \{0,1\}^{n-1}$.

## 6 Secret-Key Encryption — 20 Points

(a) Prove that no secret-key encryption scheme $\Pi = (\mathsf{Enc}, \mathsf{Dec})$ can achieve chosen-plaintext attack security in the presence of a computationally unbounded adversary (which thus can make an exponential number of encryption queries before/after being given the challenge ciphertext).

(b) Let $\mathcal{F} = \{F_k : \{0,1\}^n \to \{0,1\}^n\}_{k \in \{0,1\}^\lambda}$ be a family of pseudorandom permutations, and define a fixed-length encryption scheme $(\mathsf{Enc}, \mathsf{Dec})$ as follows: Upon input message $m \in \{0,1\}^{n/2}$ and key $k \in \{0,1\}^\lambda$ , algorithm $\mathsf{Enc}$ chooses a random string $r \leftarrow_\$ \{0,1\}^{n/2}$ and computes $c := F_k(r||m)$. Show how to decrypt, and prove that this scheme is CPA-secure for messages of length $n/2$.

## 7 Message Authentication — 25 Points

(a) Assume UF-CMA MACs exist. Prove that there exists a MAC that is UF-CMA but is not *strongly* UF-CMA, where the latter means that the attacker is allowed to forge also on messages $m^*$ that are not fresh (i.e., $m^*$ can be equal to one of the messages that were part of tagging queries), so long as the forged tag $\tau^*$ is fresh. In other words, the challenger of strong UF-CMA outputs 1 if and only if: (i) $\mathsf{Tag}(k, m^*) = \tau^*$; and (ii) $(m^*, \tau^*) \neq (m, \tau)$ for all pairs $(m, \tau)$ corresponding to tagging queries (i.e., either the message $m^*$ or the tag $\tau^*$ is fresh).

(b) Assume a generalization of MACs where a MAC $\Pi$ consists of a pair of algorithms $(\mathsf{Tag}, \mathsf{Vrfy})$, such that $\mathsf{Tag}$ is as defined in class (except that it could be randomized), whereas $\mathsf{Vrfy}$ is a deterministic algorithm that takes as input a candidate pair $(m, \tau)$ and returns a decision bit $d \in \{0,1\}$ (indicating whether $\tau$ is a valid tag of $m$).

Consider a variant of the game defining UF-CMA security of a MAC $\Pi = (\mathsf{Tag}, \mathsf{Vrfy})$, with key space $\mathcal{K} = \{0,1\}^\lambda$, where the adversary is additionally granted access to a verification oracle $\mathsf{Vrfy}(k, \cdot, \cdot)$.

(i) Make the above definition precise, using the formalism we used in class. Call the new notion "unforgeability under chosen-message and verification attacks" (UF-CMVA).

(ii) Show that whenever a MAC has unique tags (i.e., for every key $k$ there is only one valid tag $\tau$ for each message $m$) then UF-CMA implies UF-CMVA.

(iii) Show that if tags are not unique there exists a MAC that satisfies UF-CMA but not UF-CMVA.