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 13, 2019

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) Let $(\mathsf{Enc}, \mathsf{Dec})$ be a perfectly secret encryption scheme over message space $\mathcal{M}$ and key space $\mathcal{K}$, satisfying the following relaxed correctness requirement: There exists $t \in \mathbb{N}$ such that, for all $m \in \mathcal{M}$, it holds that $\Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m] \geq 2^{-t}$ (where the probability is over the choice of $k \leftarrow\!\!\$\, \mathcal{K}$). Prove that $|\mathcal{K}| \geq |\mathcal{M}| \cdot 2^{-t}$.

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 $y_1, \ldots, y_t \in \mathcal{Y}$ (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.

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

(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 λ-bit stretch. Prove that G is by itself a one-way function.

(b) Let $f : \{0,1\}^n \to \{0,1\}^n$ be a OWF. Consider the function $g : \{0,1\}^{n+\log n} \to \{0,1\}^{n+\log n+1}$ defined by $g(x||j) := (f(x), j, x_j)$, where $x := (x_1, \ldots, x_n)$, and j is interpreted as an integer in $[n]$ (i.e., $|j| = \log n$).

(i) Show that g is a OWF if f is.

(ii) Show that for every $i \in [n']$ there is a PPT algorithm $\mathcal{A}_i$ for which

$$\Pr\left[\mathcal{A}_i(g(x')) = x'_i : \; x' \leftarrow_{\$} \{0,1\}^{n+\log n}\right] \geq \frac{1}{2} + \frac{1}{2n},$$

where $x' = (x_1, \ldots, x_{n'})$.

4 Pseudorandom Generators — 20 Points

(a) Let $G_1, G_2 : \{0,1\}^\lambda \to \{0,1\}^{\lambda+\ell}$ be two deterministic functions mapping λ 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 λ 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 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. (Recall that strong unforgeability allows the attacker to produce a forgery (m^*, τ^*) such that $(m^*, \tau^*) \neq (m, \tau)$ for all messages m que)

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