Graduate Cryptography September 18, 2017

Problem Set 1

Lecturer: Daniel Wichs *Due: Sept 27, 2017*

Problem 1 (t-wise independent hash) 10 pts

A hash function $h : \mathcal{K} \times \mathcal{U} \to \mathcal{V}$ is t-wise independent if for all t distinct values $x_1, \ldots, x_t \in \mathcal{U}$ and any $y_1, \ldots, y_t \in \mathcal{V}$ we have

$$\Pr[h(K, x_1) = y_1, \ldots, h(K, x_t) = y_t] = \prod_{i=1}^{t} \Pr[h(K, x_i) = y_i] = \frac{1}{|\mathcal{V}|^t}$$

where K is a random variable that's uniform over $\mathcal{K}$.

Use the ideas we saw in class about polynomials over a finite field $\mathbb{F}$ (e.g., in the construction of one-time MACs and Shamir secret sharing) to construct such a scheme for any t with $\mathcal{K} = \mathbb{F}^t$ and $\mathcal{U} = \mathcal{V} = \mathbb{F}$.

Show how to use the above to construct a message authentication code (MAC) which can be securely used to authenticate up to $(t-1)$ messages.

Problem 2 (Two-time Security?) 10 pts

We showed that the one-time pad is a perfectly secure "one-time" encryption scheme that allows us to encrypt a single message. In this problem, we want to define two-time encryption that can be used to encrypt 2 messages and more generally t-time encryption.

Part A: Here is a natural way to define *two-time perfect secrecy* for encryption. For any two pairs of messages $(m_0, m_1) \in \mathcal{M} \times \mathcal{M}$ and $(m'_0, m'_1) \in \mathcal{M} \times \mathcal{M}$ and for any ciphertexts c_0, c_1 we have

$$\Pr[\mathsf{Enc}(K, m_0) = c_0, \mathsf{Enc}(K, m_1) = c_1] = \Pr[\mathsf{Enc}(K, m'_0) = c_0, \mathsf{Enc}(K, m'_1) = c_1]$$

Show that no encryption scheme can satisfy this definition.

Part B: To overcome the limitation in part A, we first relax the problem by considering statistical security where we require that for all $(m_0, m_1), (m'_0, m'_1) \in \mathcal{M} \times \mathcal{M}$

$$\mathsf{SD}(\ (\mathsf{Enc}(K, m_0), \mathsf{Enc}(K, m_1))\ ,\ (\mathsf{Enc}(K, m'_0), \mathsf{Enc}(K, m'_1))\ ) \leq \varepsilon$$

Show that, even with this relaxation, no encryption scheme with a deterministic encryption procedure can satisfy the above with $\varepsilon < 1$.

Part C: We relax the problem further by considering randomized encryption schemes where, for a fixed k, m the encryption procedure $\mathsf{Enc}(k, m)$ can additional randomness to create the ciphertext. We require perfect correctness so that for all $m \in \mathcal{M}, k \in \mathcal{K}$: $\Pr[\mathsf{Dec}(k, \mathsf{Enc}(k, m)) = m] = 1$ where the probability is over the randomness of the encryption procedure. Show that there exists a randomized encryption scheme that achieves the above for arbitrarily small ε.

(Hint: Use t-wise independent hash functions from the previous problem with $t = 2$. Let the encryption procedure call the hash function on a random input to derive a new " one-time pad" key on each invocation.)

Part D: Go back to part A and generalize your proof to randomized encryption schemes. In other words, show that no randomized encryption scheme can achieve statistical two-time security with $\varepsilon = 0$.

Problem 3 (Refreshing Secret Sharing) 10 pts

A secret is shared across n computers using Shamir Secret Sharing with a threshold $t \geq 2$ (t parties learn nothing, $t + 1$ can recover the secret). Every morning, a determined hacker can choose to compromise any one of the computers. The computer stays compromised for an entire day meaning that the adversary can see everything that happens on it during that day. However, by the following morning the hack is guaranteed to be discovered and the attacker is booted off from the computer. The attacker can then hack a new computer that morning (potentially the same one as the previous morning) and so it goes day after day for ever.

We want to make sure the attacker never learns the shared secret. To do so, we want to have a protocol that the n computers can run once a day to "refresh" their shares. The attacker sees everything that happens on the compromised computer during the run of the protocol. Design a protocol to solve this problem and argue that it is secure.

Problem 4 (Statistical Distance) 10 pts

Part A: Let X be uniformly random over $\{1, \ldots, n\}$ and let Y be uniformly random over $\{1, \ldots, n+1\}$. What's the statistical distance $SD(X, Y)$? If we think of n as a security parameter, are the two distributions computationally indistinguishable (justify your answer)?

Part B: Show that for any function $G : \{0,1\}^n \to \{0,1\}^{n+1}$ the statistical distance between $G(U_n)$ and U_{n+1} is at least $1/2$ where U_ℓ denotes the uniform distribution over $\{0,1\}^\ell$.

Part C: Show that statistical distance obeys the triangle inequality: $SD(X,Z) \leq SD(X,Y) + SD(Y,Z)$.

Part D: Show that for any function f and any random variables X, Y we have $SD(f(X), f(Y)) \leq SD(X,Y)$.

Problem 5 (Alternate Definition) 10 pts

Our definition of one-time computationally secure encryption considered two games $OneSec^b$ with $b = 0, 1$ which we required to be computationally indistinguishable. An alternate definition considers a single game $AltOneSec(n)$ which proceeds as follows:

- The adversary $A(n)$ chooses messages m_0, m_1 and gives them to the challenger
- The challenger chooses a uniformly random bit $b \leftarrow \{0,1\}$ and key $k \leftarrow \{0,1\}^n$. It encrypts the message m_b by setting $c = \mathsf{Enc}(k, m_b)$ and gives c to the adversary.
- The adversary outputs a "guess" b' and the game outputs 1 if $b = b'$ and 0 otherwise.

For an adversary A, we define $AltOneSec_A(n)$ to be a random variable denoting the output of the above game when played with A. An encryption scheme is then defined to be secure if for all PPT A there is some negligible ε such that $|\Pr[AltOneSec_A(n) = 1] - \frac{1}{2}| = \varepsilon(n)$.

Show that the alternate definition is equivalent to the one we gave in class, meaning that a scheme is secure according to one definition if and only if it is secure according to the other one.