Problem Set 7

Problem 1: Not a PRF

Consider the keyed function $H : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^{2n}$ defined as: $H_k(x) = G(k) \oplus G(x)$, where $G : \{0,1\}^n \to \{0,1\}^{2n}$ is a pseudorandom generator.

(a) Describe and formally analyze an explicit attack showing that H is not a PRF.

(b) Is there a successful attack making a single query that distinguishes H_k (for random k) from a random function $f : \{0,1\}^n \to \{0,1\}^{2n}$? Why or why not?

Problem 2: A randomized variable-length MAC from a PRF

Let F be a pseudorandom function. Show that the following MAC is insecure for variable-length messages. Gen outputs a uniform $k \in \{0,1\}^n$. Let $\langle i \rangle$ denote an $n/2$-bit encoding of the integer i.

To authenticate a message $m = m_1 \| \dots \| m_\ell$, where $m_i \in \{0,1\}^{n/2}$, choose a uniform $r \leftarrow \{0,1\}^n$, compute $t := F_k(r) \oplus F_k(\langle 1 \rangle \| m_1) \oplus \cdots \oplus F_k(\langle \ell \rangle \| m_\ell)$ and let the tag be (r,t).

Problem 3: Cryptographic Mechanisms

For each of the following, identify the most appropriate cryptographic mechanism(s) (from among private-key encryption, pseudorandom generators, pseudorandom functions, message authentication codes, hash functions, public-key encryption, or digital signatures) for addressing the problem. Points will be deducted if you list extraneous mechanisms. **Explain your answer in 1-2 sentences.**

(a) A company wants to distribute authenticated software updates to its customers.

(b) A user wants to ensure secrecy of the files stored on his hard drive.

(c) A customer wants to send his credit card number (confidentially) to a merchant over the web to complete a purchase.

(d) A general wants to send a message to a lieutenant, and wants to ensure both confidentiality and integrity.

(e) A client wants to store a short record of a large file he uploads to a server, so that the client can verify that the file has not been altered when it downloads the file later.

(f) A user needs 1,000,000 random bits in order to run a simulation, but obtaining truly random bits is expensive.

Problem 4: Mode of Encryption

Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and consider the following mode of encryption: to encrypt an ℓ-block message $m_1, \dots, m_\ell$ using key k, choose uniform $c_0 \in \{0,1\}^n$ and then for $i = 1, \dots, \ell$ set $c_i := F_k(m_i) \oplus c_{i-1}$. Output the ciphertext $c_0, \dots c_\ell$.

(a) How would decryption of a ciphertext $c_0, \dots, c_\ell$ be done?

(b) Is this scheme EAV-secure? If yes, give a proof; if not, describe an explicit attack.

(c) Is this scheme CPA-secure? Provide a brief justification of your answer.

Problem 5: Breaking El Gamal Encryption with a Quantum Computer

Recall that the El Gamal encryption scheme is given as follows: The key generation algorithm Gen on input 1^n generates a triple (G, q, g) where G is a cyclic group of order q and g is a generator of G. Then it chooses a uniform $x \leftarrow \mathbb{Z}_q$ and computes $h = g^x$. The public key is (G, q, g, h) and the private key is (G, q, g, x). The encryption algorithm Enc: on input a public key (G, q, g, h) and message m, chooses a uniform $y \leftarrow \mathbb{Z}_q$ and outputs $\langle g^y, h^y \cdot m\rangle$. Decryption Dec: on input private key (G, q, g, x) and ciphertext $\langle c_1, c_2\rangle$ computes $\hat{m} = c_2/c_1^x$.

(a) Give a sufficient condition under which the El Gamal scheme is CPA secure.

(b) Assume you have oracle access to a quantum computer that can efficiently calculate discrete logarithms in G with respect to the generator g. Give an explicit CPA attacker on this scheme.

For the next two subexercises, consider the specific case of the cyclic group $\mathbb{G} = \mathbb{Z}_{37}^*$ with generator $g = 2$. Assume $x = 6$ is chosen during the key generation.

(c) What are the actual values of q and h in the resulting public key $\mathsf{pk} = \langle \mathbb{G}, q, g, h\rangle$? Show your calculations.

(d) Using the public key from the previous part, encrypt the message $m = 7$. You can assume any randomness y that you want.

Problem 6: Padded RSA

Let $\tilde{\Pi} = (\tilde{\mathsf{Gen}}, \tilde{\mathsf{Enc}}, \tilde{\mathsf{Dec}})$ be the plain RSA encryption scheme for $2n$ bit messages, and consider the padded encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ where $\mathsf{Gen} = \tilde{\mathsf{Gen}}$. To encrypt a plaintext $m \in \{0,1\}^n$, sample $r \leftarrow \{0,1\}^n$ and output $\tilde{\mathsf{Enc}}_{\mathsf{pk}}(m\|r)$. Decryption is done by decrypting with $\tilde{\mathsf{Dec}}_{\mathsf{sk}}$ and outputting the first half of the resulting string.

(a) Find a chosen-ciphertext attack on Π. Give a precise description of an adversary $\mathcal{A}$, using the notation introduced for the indistinguishability experiments. Avoid imprecise verbose descriptions. Calculate the success probability $\mathcal{A}$.