Problem Set 7

Problem 1: RSA Signatures

(a) Consider the plain RSA signature scheme with modulus $N = 85 = 5 \cdot 17$.

1. Compute $\phi(N)$.
2. Say the public exponent is $e = 5$. Find the private exponent d. (Hint: look at the sequence $\phi(N)+1, 2\cdot\phi(N)+1, \ldots$ until you find a multiple of e.)
3. Compute the signature on the message 3.
   Hint: Note that $[3^4 \mod 85] = [81 \mod 85] = [(-4) \mod 85]$.

(b) Consider a *padded* RSA signature scheme, where to sign a message $m \in \{0,1\}^{80}$ the signer chooses random r with $r\|m < N$ (where $\|$ denotes concatenation), computes $\sigma = [(r\|m)^d \mod N]$, and outputs signature σ.

1. How would verification be done?
2. Is this scheme secure? If yes, give a 1-2 sentence explanation; if not, show an attack.

Problem 2: 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 3: 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 $m = m_1\| \ldots \|m_\ell$, 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 4: 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 5: 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 $m_1, \ldots, m_\ell$ using key k, choose uniform $c_0 \in \{0,1\}^n$ and then for $i = 1, \ldots, \ell$ set $c_i := F_k(m_i) \oplus c_{i-1}$. Output the ciphertext $c_0, \ldots c_\ell$.

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

(b) Describe and analyze an explicit attack showing that this scheme is not EAV- secure.

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

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 $\mathcal{A}$.