Name: _____
ID: _____
Grade: _____
05/12/2011

Factoring, RSA, Discrete Log, Diffie-Hellman, Key Management, Public Key, El Gamal, TDP, Digital Signatures, ROM

7.1 Let $\mathbb{G}$ be an abelian group. Prove that there is a *unique* identity in $\mathbb{G}$, and that every element $g \in \mathbb{G}$ has a *unique* inverse.

■

7.2 This question concerns the Euler phi function.

(a) Let p be a prime and $e \geq 1$ an integer. Show that $\phi(p^e) = p^{e-1}(p-1)$.

(b) Let p, q be relatively prime. Show that $\phi(pq) = \phi(p) \cdot \phi(q)$. (You may use the Chinese remainder theorem.)

(c) Prove Theorem: $N = \prod_i p_i^{e_i}$, $\{p_i\}$ are distinct primes, $\phi(N) = \prod_i p_i^{e_i-1}(p_i - 1)$.

■

7.3 Solve the following system of congruences (find x by hand):

$$13x \equiv 4 \pmod{99}, \qquad 15x \equiv 56 \pmod{101}$$

■

7.4 Compute $[101^{4,800,000,023} \bmod 35]$ (by hand).

■

7.5 Prove that if $\mathbb{G}, \mathbb{H}$ are groups, then $\mathbb{G} \times \mathbb{H}$ is a group.

■

7.6 Let $N = pq$ be a product of two distinct primes. Show that if $\phi(N)$ and N are known, then it is possible to compute p and q in polynomial time.

■

7.7 Prove formally that the hardness of the CDH problem relative to $\mathcal{G}$ implies the hardness of the discrete logarithm problem relative to $\mathcal{G}$.

■

9.1 Consider the following key-exchange protocol:

1. Alice chooses $k, r \leftarrow \{0,1\}^n$ at random, and sends $s := k \oplus r$ to Bob.
2. Bob chooses $t \leftarrow \{0,1\}^n$ at random and sends $u := s \oplus t$ to Alice.
3. Alice computes $w := u \oplus r$ and sends w to Bob.
4. Alice outputs k and Bob computes $w \oplus t$.

Show that Alice and Bob output the same key. Analyze the security of the scheme (i.e. either prove its security or show a concrete attack by an eavesdropper).

■

10.1 Assume a public-key encryption scheme for single-bit messages. Show that, given pk and a ciphertext c computed via $c \leftarrow \mathsf{Enc}_{pk}(m)$, it is possible for an unbounded adversary to determine m with probability 1. This shows that perfectly-secret public-key encryption is impossible.

■

10.2 Say a deterministic public-key encryption scheme is used to encrypt a message m that is known to lie in a small set of $\mathcal{L}$ possible values. Show how it is possible to determine m in time linear in $\mathcal{L}$ (assume that encryption of an element takes a single unit of time).

■

10.3 In multiple message eavesdropping experiment in public-key encryption, when $t = 2$ (two messages in each vector of messages), prove that there exists a negligible function negl such that $\frac{1}{2} + \mathsf{negl}(n) \geq \frac{1}{2} \cdot \Pr[\mathcal{A}(c_0^1, c_1^2) = 0] + \frac{1}{2} \cdot \Pr[\mathcal{A}(c_1^1, c_1^2) = 1]$. (see Page 8 in 8.2pubkey-RSA.pdf)

■

10.4 Consider the following public-key encryption scheme. The public key is $(\mathbb{G}, q, g, h)$ and the private key is x, generated exactly as in the El Gamal encryption scheme. In order to encrypt a bit b, the sender does the following:

- If $b = 0$ then choose a random $y \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = h^y$. The ciphertext is $\langle c_1, c_2 \rangle$.
- If $b = 1$ then choose independent random $y, z \leftarrow \mathbb{Z}_q$ and compute $c_1 = g^y$ and $c_2 = g^z$, and set the ciphertext is $\langle c_1, c_2 \rangle$.

(a) Show that it is possible to decrypt efficiently given knowledge of x.

(b) Prove that this encryption scheme is CPA-secure if the decisional Diffie-Hellman problem is hard relative to $\mathcal{G}$.

■

10.5 Suppose that the RSA Assumption fails "somewhat" on a particular composite number N and e with $\gcd(e, \phi(N)) = 1$, in the sense that there is a t-time algorithm $\mathcal{A}$ such that

$$\Pr[\mathcal{A}(x^e) = x \pmod N] > 0.01$$

Show that there is a $100(\log N)^{100} \cdot t$-time algorithm $\mathcal{A}'$ that breaks the RSA Assumption completely for N, e in the sense that

$$\Pr[\mathcal{A}'(x^e) = x \pmod N] > 0.99$$

Hint: Use the fact that $y^{1/e} r = (yr^e)^{1/e} \pmod N$ for every $r \in Z_N^*$.

■

10.6 The natural way of applying hybrid encryption to the El Gamal encryption scheme is as follows. The public key is $pk = \langle \mathbb{G}, q, g, h \rangle$ as in the El Gamal scheme, and to encrypt a message m the sender chooses random $k \leftarrow \{0,1\}^n$ and sends

$$\langle g^r, h^r \cdot k, \mathsf{Enc}_k(m) \rangle,$$

where $r \leftarrow \mathbb{Z}_q$ is chosen at random and Enc represents a private-key encryption scheme. Suggest an improvement that results in a shorter ciphertext containing only a *single* group element followed by a private-key encryption of m.

■

10.7 Let $\widehat{\Pi} = (\widehat{\mathsf{Gen}}, f)$ and hc be as in Construction 1. (See Page 5 in 10tdp-rom.pdf)

- Gen: as in Construction 1.
- Enc: on input a public key I and a message $m \in \{0,1\}$, choose a random $x \leftarrow \mathcal{D}_I$ such that $\mathsf{hc}_I(x) = m$, and output the ciphertext $f_I(x)$.
- Dec: on input a private key td and a ciphertext y with $y \in \mathcal{D}_{\mathsf{td}}$, compute $x := f_I^{-1}(y)$ and output the message $\mathsf{hc}_I(x)$.

(a) Argue that encryption can be performed in polynomial time, while ensuing that correctness holds with all but negligible probability.

(b) Prove that if $\widehat{\Pi}$ is a family of trapdoor permutations and hc is a hard-core predicate of $\widehat{\Pi}$, then this construction is CPA-secure.

■

12.1 Prove that the existence of a one-time signature scheme for 1-bit messages implies the existence of one-way function.

■

12.2 For each of the following variants of the definition of security for signatures, state whether textbook RSA is secure and prove your answer:

(a) In this first variant, the experiment is as follows: the adversary is given the public key pk and a random message m. The adversary is then allowed to query the signing oracle once on a single message that does not equal m. Following this, the adversary outputs a signature σ and succeeds if $\mathsf{Vrfy}_{pk}(m, \sigma) = 1$. As usual, security is said to hold if the adversary can succeed in this experiment with at most negligible probability.

(b) The second variant is as above, except that the adversary is not allowed to query the signing oracle at all.

■

12.3 Consider the Lamport one-time signature scheme. Describe an adversary who obtains signatures on two messages of its choice and can then forge signatures on any message it likes.

■

13.1 Prove that the pseudorandom function construction (see Page 11 in 10tdp-rom.pdf) is indeed secure in the random oracle model.

■