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

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

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

■

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.

■

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).

■

10.6 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.

■

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.

■