HIT — Cryptography — Homework 5

November 24, 2016

Problem 1. Compute $[101^{4,800,000,023} \bmod 35]$ (by hand).

Problem 2. 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.

Problem 3. For an RSA public key $\langle N, e\rangle$, we have an algorithm $\mathcal{A}$ that always correctly computes $LSB(x)$ given $[x^e \mod N]$. Write full pseudocode for an algorithm that computes x from $[x^e \mod N]$.

Problem 4. 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).

Problem 5. 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 $\mathcal{G}$

Problem 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.

Problem 7. 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.

Problem 8. 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.