Cryptography, homework sheet 4

Due for 2MMC10: 05 October 2017, 10:45

and for Mastermath: 09 November 2017, 10:45 by email to `crypto.course@tue.nl`

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. Do not email Tanja your homework or put homework in mailboxes.

1. Use the Rabin test (see below) to prove that $x^4 + x + 1$ is irreducible over $\mathbb{F}_2$. You should be able to do this exercise by hand. Please document the results of all steps in the algorithm and show how they were obtained.

2. In this exercise you should argue about the formal security properties of hash functions and find security reductions.

   (a) Let h be a one-way permutation. Let $H = h \circ h$ be the function resulting from applying h twice, i.e., $H(m) = h(h(m)$. Show that H is preimage resistant if h is preimage resistant. To prove this, assume you are given A that breaks PRE for H. Show that it breaks PRE for h.

   (b) Let $h_1 : \{0,1\}^* \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^* \to \{0,1\}^{n_2}$ be hash functions. Show that the combined hash function $H : \{0,1\}^* \to \{0,1\}^{n_1+n_2}, m \mapsto h_1(m)||h_2(m)$ is collision resistant if at least one of h_1 and h_2 is collision resistant.

   (c) Let $h_1 : \{0,1\}^* \to \{0,1\}^{n_1}$ and $h_2 : \{0,1\}^* \to \{0,1\}^{n_2}$ be hash functions. Show that collision resistance of h_1 does not imply collision resistance of the combined hash function $H : \{0,1\}^* \to \{0,1\}^{n_1}, m \mapsto h_1(h_2(m))$.

3. Sometimes an attacker gets to attack multiple targets at once and is satisfied breaking any *one* of them. For hash functions multi-target preimage attacks are interesting. We speak of a k-target preimage attack if the attacker is given the outputs $h(m_1), h(m_2), \ldots, h(m_k)$ but not the inputs $m_1, m_2, \ldots, m_k$ of a hash function $h : \{0,1\}^* \to \{0,1\}^n$ and has the goal of finding some (i, x) so that $h(x) = h(m_i)$.

   (a) Find an attack that takes time $2^n/k$ to succeed in finding such an (i, x) with high probability.

   (b) Show that a k-target preimage attack A succeeding with probability p can be turned into a 1-target preimage attack, i.e., a regular preimage attack, taking the same time as A and succeeding with probability p/k.

4. $3 \in \mathbb{F}^*_{1013}$ generates a group of order 1012, so it generates the whole multiplicative group of the finite field.

   Alice's public key is $h_a = 224$. Use ElGamal encryption to encrypt the messge $m = 42$ to her using the "random" value $r = 654$.

   You now may write the result of $a^b \bmod n$ in one go, without stating intermediate results – but it should be clear what computation you did.

5. You find two signatures made by Alice. You know that she is using the ElGamal signature scheme over $\mathbb{F}_{2027}$ and that the order of the generator is $n = 1013$. The signatures are for $h(m_1) = 345$ and $h(m_2) = 567$ and are given by $(r_1, s_1) = (365, 448)$ and $(r_2, s_2) = (365, 969)$. Compute (a candidate for) Alice's long-term secret a based on these signatures, i.e. break the system.

Hint: There is a reason that I don't state the generator or Alic'e public key; you're not supposed to compute the DL. ElGamal in the subgroup works the same as described in the lecture; the only difference is that s is computed modulo the order of the subgroup (which is prime here, so that everything is nicely invertible).

Here is a formal statement of the Rabin test:

Lemma 1 (Rabin test)
The polynomial $f(x) \in \mathbb{F}_q[x]$ of degree $\deg(f) = m$ is irreducible if and only if

$$f(x) | x^{q^m} - x$$

and for all primes d dividing m one has

$$\gcd(f(x), x^{q^{m/d}} - x) = 1.$$