CSE 5852: Problem Set 8

Due: November 28, 2016

In this assignment you'll be doing be working with composite moduli and considering security definitions for signatures.

1 The group $\mathbb{Z}_n^*$

Assume that $p = 5, q = 7$ and $N = pq = 35$.

1. **5 pts** How many elements are in $\mathbb{Z}_N^*$?
2. **15 pts** What are the elements of $\mathbb{Z}_N^*$?
3. **10 pts** For each element of $\mathbb{Z}_N^*$ what is its inverse? **Hint:** I recommend putting this question and the previous one in a large table.

2 The RSA problem

As in the previous problem consider the setting where $p = 5, q = 7$ and $N = pq = 35$.

1. **5 pts** What is $\phi(N)$?
2. **15 pts** Recall the RSA problem requires finding an $e > 1$ such that $\gcd(e, \phi(N)) = 1$. How many possible values for e are there between 2 and $\phi(N)$? What are they?
3. **5 pts** Compute d for each possible e. Recall that d is e's inverse $\mod \phi(N)$.
4. **15 pts** For one e, d pair show the computation using the extended Euclid algorithm for computing the gcd. This algorithm is below. Remember if your output is negative you need to add $\phi(N)$ to make sure its between 1 and $\phi(N)$. I recommend using a table of the following form:

α	β	r	α_2	β_2	r_2	t
0	1	e	1	0	$\phi(N)$	

The extended Euclidean algorithm takes input $gcd(a, b)$ and outputs α, β, z such that $a\alpha + b\beta = z$ and $z = gcd(a, b)$. This algorithm runs in polynomial time in the size of the inputs.

Extended Euclidean Algorithm

(a) Input a, b.
(b) Set $\alpha = 0, \beta = 1, r = b$.
(c) Set $\alpha_2 = 1, \beta_2 = 0, r_2 = a$.
(d) While $r \neq 0$:
  i. $t = r_2/r$.
  ii. $(r_2, r) = (r, r_2 - t \cdot r)$.
  iii. $(\alpha_2, \alpha) = (\alpha, \alpha_2 - t \cdot \alpha)$.
  iv. $(\beta_2, \beta) = (\beta, \beta_2 - t \cdot \beta)$.
(e) Output (α_2, β_2, r_2).

3 Definitions of Signatures

In class we presented the following signature definition called existentially unforgeable under chosen message attack.

$\mathtt{EU} - \mathtt{CMA}_{\mathsf{Gen},\mathsf{Sig},\mathsf{Vfy},\mathcal{A}}(1^n)$:

1. Run $(vk, sk) \leftarrow \mathsf{Gen}(1^n)$.
2. Give vk to $\mathcal{A}$.
3. For $i = 1$ to k:

   Receive m_i from $\mathcal{A}$.

   Provide σ_i to $\mathcal{A}$.
4. Receive m', σ' from $\mathcal{A}$.
5. Output 1 if and only if $\mathsf{Vfy}(vk, m', \sigma') = 1$.

Definition 1. *A signature scheme* $(\mathsf{Gen}, \mathsf{Sig}, \mathsf{Vfy})$ *is existentially unforgeable under chosen message attack if for all PPT* $\mathcal{A}$ *there exists a negligible* $\epsilon(n)$ *such that*

$$\Pr[\mathtt{EU} - \mathtt{CMA}_{\mathsf{Gen},\mathsf{Sig},\mathsf{Vfy},\mathcal{A}}(1^n) = 1] < \epsilon(n).$$

Consider the setting where the sender signs only random messages. We will still consider a forgery if the adversary is able to produce a signature on an arbitrary message. We will call this setting **existentially-unforgeable under random message attack** or EU-RMA.

1. **10 pts** Provide an experiment and definition for EU-RMA.
2. **20 pts** Show that EU-CMA security implies EU-RMA security. That is show that if there exists a PPT $\mathcal{A}$ that forges in the EU-RMA game with probability $1/p(n)$ for some polynomial $p(n)$ there there is a PPT $\mathcal{A}'$ that forges in the EU-CMA game with an inverse polynomial probability. **Explicitly describe the behavior of $\mathcal{A}'$ and how it uses $\mathcal{A}$.**