Institut for Matematik og Datalogi
Syddansk Universitet

November 18, 2016
JFB

Cryptology – E16 – Lecture 15

Announcement

Vi har netop opslået instruktorater for foråret. Alle der er interesserede opfordres til at søge. Det er skulle forklare stoffet for andre er en virkelig god måde at øge sin egen forståelse på. Det gælder ikke blot det stof man skal gennemgå (og derfor kunne godt), men gennem at man skal forklare for andre, bliver man også bedre til at finde ind til kernen i problemer og dermed bliver man selv bedre til at studere. Fristen for at søge er 28/11 og opslaget kan ses dels omkring på IMADA samt via SDU ledige stillinger.

The deadline for applying for TA positions at IMADA is November 28.

Announcement

The next pizza meeting will be held starting at 16:00 in U163 on November 23.

Lecture, November 15

We continueed with chapter 16, covering up through section 16.5.2. We also covered sections 4.1, 4.2, 4.3, and 4.5, with emphasis on curves of characteristic $p > 3$.

Lecture, November 21

We will cover section 16.5.3 from chapter 16 and begin on chapter 19.

Lecture, November 28

We will begin on chapter 21.

Problem session November 22

1. A common way to speed up RSA decryption incorporates the Chinese remainder theorem, as follows. Suppose that $d_K(y) = y^d \pmod{n}$ and $n = p \cdot q$. Define $d_p = d \pmod{(p-1)}$ and $d_q = d \pmod{(q-1)}$; and let $M_p = q^{-1} \pmod{p}$ and $M_q = p^{-1} \pmod{q}$. Then consider the following algorithm:

   ```
   Algorithm CRT-Optimized RSA Decryption($n, d_p, d_q, M_p, M_q, y$)

   $x_p \leftarrow y^{d_p} \pmod{p}$
   $x_q \leftarrow y^{d_q} \pmod{q}$
   $x \leftarrow M_p q x_p + M_q p x_q \pmod{n}$
   return($x$)
   ```

   This algorithm replaces an exponentiation modulo n by modular exponentiations modulo p and q. If p and q are ℓ-bit integers and exponentiation muldulo an ℓ bin integer takes time $c\ell^3$, then the time to perform the required exponentiation(s) is reduced from $c(2\ell)^3$ to $2c\ell^3$, a savings of 75%. The final step, involving the Chinese remainder theorem, requires time $O(\ell^2)$ if d_p, d_q, M_p, and M_q have been pre-computed.

   (a) Prove that the value x returned by the algorithm is, in fact, $y^d \pmod{n}$.

   (b) Given that $p = 1511$, $q = 2003$ and $d = 1234577$, compute d_p, d_q, M_p, and M_q.

   (c) Given the above values of p, q, and d, decrypt the ciphertext $y = 152702$ using the algorithm.

   (Problem 5.13 in CTP.)

2. Consider the ElGamal Public-key Cryptosystem in $\mathbb{Z}_p^*$.

   (a) Suppose that Bob encrypted several messages, $x_1, x_2, ..., x_n$, to send to Alice using Alice's public key, but used the same value k in every encryption. Thus, the encryptions are

   $$(g^k, x_1 h^k), (g^k, x_2 h^k), ..., (g^k, x_n h^k),$$

where all operations are performed modulo p. Suppose that x_5 was also sent to the eavesdropper, Eve. How can Eve determine the other x_i's?

(b) Suppose that, instead of using the same value k, Bob used consecutive values of k. Thus, for some k the encryptions are

$$(g^k, x_1h^k), (g^{k+1}, x_2h^{k+1}), ..., (g^{k+n-1}, x_nh^{k+n-1}),$$

where all operations are performed modulo p. How can Eve still determine the other x_i's if she is sent x_5?

3. Suppse that E is an elliptic curve defined over $\mathbb{Z}_p$, where $p > 3$ is prime. Suppose that the number of points in E is a prime q, $P \in E$, and $P \neq (O)$. Prove that the discrete logarithm $\log_P(-P) = q - 1$.

4. Consider the "Naive" RSA Signature Scheme.

   (a) Demonstrate an existential forgeability attack on the (naive) RSA signature scheme, assuming that the adversary has seen signatures on two different messages.

   (b) If the adversary has only seen one signature, but is able to get a signature on one more message of its choice, show how it can perform selective forgeries.

5. In the Schnorr signature scheme, G is a public finite abelian group generated by an element g of prime order q. How could you find such a G and g if you wanted to work modulo some prime p. (Also what relation do you need between q and p.)