Institut for Matematik og Datalogi
Syddansk Universitet

November 15, 2019
JFB

Cryptology – 2019 – Lecture 15

Announcements

1. All lectures on Thursdays will start at 16:10, instead of 16:15.
2. Lecture on Thursday, November 21, is cancelled.
3. The next pizza meeting will be held starting at 16:00 on November 18.
4. The deadline for applications for TAships at IMADA for spring is November 21:

   https://www.sdu.dk/da/service/ledige_stillinger/1071043

Lecture, November 11

We started on chapter 16, covering section 16.1.1 on the Goldwasser-Micali cryptosystem. We also introduced the discrete logarithm problem in $\mathbb{Z}_p^*$, including the Pohlig-Hellman algorithm from section 3.2. The are slides on the course homepage.

Lecture, November 14

We will continue with chapter 16 and section 3.1, covering the El Gamal cryptosystem. We will also cover subsection 11.7.2 section 15.2 and subsections 18.4.2 and 18.4.3. covering up through section 16.5, and cover sections 4.1, 4.2, 4.3, and 4.5, with emphasis on curves of characteristic $p > 3$.

Lecture, November 19

We will continue with chapter 16, covering up through section 16.5.3. We may begin on chapter 19.

Problem session November 18

We will finish any problems not finished on November 12.

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 $n = pq$. 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 bit 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 Alices 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_is?

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

$$(g^k, x_1 h^k), (g^{k+1}, x_2 h^{k+1}), ..., (g^{k+n-1}, x_n h^{k+n-1}),$$

   where all operations are performed modulo p. How can Eve still determine the other x_is 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 $P \neq \mathcal{O}$. 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.)

6. I may lecture at the end.