MAT-52600 Matemaattinen kryptologia Tentti 3.10.2012

Tentaattori: Keijo Ruohonen

Huom! Mukana ei saa olla kirjallisuutta, tietokoneita eikä taulukoita. Funktiolaskin on sallittu.

1. Selosta lyhyesti klassisia kryptosysteemejä AFFINE ja HILL, niiden toimintaa ja murtomahdollisuuksia.

2. Miten kerrotaan, jaetaan ja korotetaan korkeaan potenssiin suuria lukuja modulo n, missä n:kin on suuri luku? Miten vaativia nämä operaatiot ovat?

3. **a)** n on pariton positiivinen luku. Miksi $(2^{-1}, \bmod n)$ on silloin olemassa ja mikä se on?

b) Yleisemmin, jos $n \equiv a \mod b$ ja $(a^{-1}, \bmod n)$ on olemassa niin $(b^{-1}, \bmod n)$ on myös olemassa. Mikä se on?

4. Tarkastellaan RSA-systeemiä tavallisine suurine alkulukuineen p ja q ja aukikerrottuine tuloineen $n = pq$. Jos kryptauseksponentti on $a = 3$ ja ulkopuolinen taho E saa kryptattuna kaksi viestiä w (kryptattuna c_1) ja $w + m$ (kryptattuna c_2), missä m on pienehkö tunnettu luku, niin hän voi yrittää löytää w:n ns. *Franklin–Reiter-hyökkäyksellä:*

1. Merkitään $p_1 = x^3 - c_1$ ja
$$p_2 = (x+m)^3 - c_2 = x^3 + 3mx(x+m) + m^3 - c_2.$$
Ideana on yrittää ratkaista x kongruensseista $p_1 \equiv 0$ ja $p_2 \equiv 0$ modulo n, tai sitten löytää p ja q.
2. Lasketaan
$$p_3 = p_2 - p_1 = 3mx(x+m) + c_3 \ , \quad \text{missä } \ c_3 = m^3 + c_1 - c_2.$$
3. Lasketaan
$$p_4 = 3mp_1 - (x-m)p_3 = \big(3m^3 - c_3\big)x + m(c_3 - 3c_1)$$
ja ratkaistaan x kongruenssista $p_4 \equiv 0 \mod n$, jos mahdollista. Silloin $w = x$.

Milloin hyökkäys onnistuu ja miksi?

(Franklin–Reiter-hyökkäys on yksi syy, miksi 3 ja muut pienet kryptauseksponentit eivät ole niin yleisiä pienissä laitteissa kuin luulisi.)

5. Selosta ELGAMAL-kryptosysteemiä, sen rakennetta ja toimintaa.

In English ⟶⟶⟶

MAT-52606 Mathematical Cryptology Exam 3.10.2012

Examiner: Keijo Ruohonen

Please note! This is a closed-book exam. Non-programmable calculators are allowed.

1. Describe briefly the classical cryptosystems AFFINE and HILL, how they work and how they can be broken.

2. How do you multiply, divide and raise to high powers large numbers modulo n where n, too, is large? How demanding are these operations computationally?

3. **a)** Suppose n is an odd positive number. Why does $(2^{-1}, \bmod n)$ then exist and what is it?

b) More generally, if $n \equiv a \mod b$ and $(a^{-1}, \bmod n)$ exists, then $(b^{-1}, \bmod n)$ exists, too. What is it?

4. Consider RSA with the usual two large primes p and q and $n = pq$. If the encrypting exponent is $a = 3$ and an adversary E intercepts two encrypted messages w (encrypted as c_1) and $w + m$ (encrypted as c_2), where m is a known smallish number, then she may try to find w using the so-called *Franklin–Reiter attack:*

1. Denote $p_1 = x^3 - c_1$ and
$$p_2 = (x+m)^3 - c_2 = x^3 + 3mx(x+m) + m^3 - c_2.$$
The idea is to try to solve the two equations $p_1 \equiv 0$ and $p_2 \equiv 0$ modulo n for x, or find p and q.
2. Calculate
$$p_3 = p_2 - p_1 = 3mx(x+m) + c_3 \ , \quad \text{where } c_3 = m^3 + c_1 - c_2.$$
3. Calculate
$$p_4 = 3mp_1 - (x-m)p_3 = \big(3m^3 - c_3\big)x + m(c_3 - 3c_1)$$
and solve the equation $p_4 \equiv 0$ modulo n for x, if possible. Then $w = x$.

When does the attack work and why?

(The Franklin–Reiter attack is one of the reasons why 3 and other small encrypting exponents are not as popular in small devices as one might expect.)

5. Explain the ELGAMAL cryptosystem, its working and structure.

Suomeksi ⟶⟶⟶