Some slides for 18th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

25-04-2014

Public-key crytography (from Wikipedia)

- The key used to encrypt a message is not the same as the key used to decrypt it.
- Each user has a pair of cryptographic keys-a public key and a private key. The private key is kept secret, while the public key may be widely distributed.
- Messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.
- The keys are related mathematically, but the private key cannot feasibly (ie, in actual or projected practice) be derived from the public key.
- The discovery of algorithms that could produce public/private key pairs revolutionized the practice of cryptography beginning in the middle 1970s.

[Wikipedia]

You considered RSA in previous semesters. We will consider another cryptosystem in Algebra 2:

1. ElGamal,

ElGamal is nowadays used in practice. It has been improved using elliptic curves: it has smaller key sizes and faster operations. New standards are coming.

ElGamal

Based on discrete logarithm problem:

Given a prime p and $y, g \in \mathbb{N}$, find x such that

$$y \equiv g^x \pmod{p}$$

1. Alice and Bob choose p, a big prime, and $g \in \mathbb{N}$ s.t. $0 < g < p$ and g has order $p-1$ in $(\mathbb{Z}/p\mathbb{Z})^*$ (a generator of $(\mathbb{Z}/p\mathbb{Z})^*$)
2. Alice chooses a, with $0 < a < p$ and computes $[g^a]_p$.
   Secret Key=a
   Public Key=$[g^a]_p$
3. Bob chooses b with $0 < b < p$ and computes $[g^b]_p$.
   Secret Key=b
   Public Key=$[g^b]_p$

4. Alice wants to send a message m, $0 < m < p$ to Bob. She sends:

$$\left([g^a]_p, [m(g^b)^a]_p\right)$$

5. Bob gets $([x_1]_p, [x_2]_p)$ and computes

$$[x_2]_p([x_1^b]_p)^{-1} = [mg^{ab}]_p([g^{ab}]_p)^{-1} = [m]_p$$

   and since $m < p$ he can recover m.

To encrypt the message one uses the public key of the receiver and the secret key of the sender.

6. Eve?: she had to compute b from $[g^b]_p$

Lemma 4.8.3

Let τ, d and n be natural numbers, where $\tau > 1$. Then $\tau^d - 1$ divides $\tau^n - 1$ if and only if d divides n.

$$X^{p^n} - X = X(X^{p^n-1} - 1) = X \prod_{d \mid p^n-1} \Phi_d$$

Theorem 4.8.8

The polynomial $X^{p^n} - X \in \mathbb{F}_p[X]$ is the product

$$X^{p^n} - X = f_1 \cdots f_r$$

of the monic irreducible polynomials $f_1, \ldots, f_r$ in $\mathbb{F}_p[X]$ of degree d, where $1 \leq d \leq n$ and $d \mid n$.

Corollary 4.8.9

Let N_d denote the number of monic irreducible polynomials of degree d in $\mathbb{F}_p[X]$. Then

$$p^n = \sum_{d \mid n} dN_d$$