Advanced Cryptography

May 31, 2022

1. *ADDITIVE Elgamal* modulo $n = 64$ generated by $g = 33$.

   (a) Alice has the secret key $x = 5$. Bob has the temporary key $y = 6$. Compute the public key of Alice. Show how Bob encrypts the message $m = 7$ and how Alice gets back the clear message. (2P)

   (b) Agent Eve computes $g^{-1} \bmod n$ and finds Alice's secret key using her public key. Make the computations. (2P)

2. *MULTIPLICATIVE Elgamal* modulo $p = 19$ in the group generated by $g = 2$. Alice has the public key $h = 6$. Bob sends the encrypted message $(c_1, c_2) = (15, 18)$. Decrypt the message. (4P)

3. *RSA.* A message m modulo 91 is encrypted with the public key $e = 5$. The result is $c = 10$. Decrypt the message using the function $\lambda(N)$. (4P)

4. *Goldwasser-Micali.* A message encrypted modulo 133 reads 81, 52, 74, 59. Decrypt the message. (4P)

5. *Shamir's No Key Protocol.* Alice sends to Bob the message $m = 5$ using $p = 17$. Alice's secret key is $a = 7$ and Bob's secret key is $b = 9$. Compute the protocol.

6. *Shamir's Secret Sharing.* Let $P \in \mathbb{Z}_{19}[X]$ a polynomial of degree 2. Consider the following pairs $(\alpha, P(\alpha))$ with $\alpha \in \mathbb{Z}_{19} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{19}$: $(10, 13)$, $(11, 0)$ and $(12, 10)$. Deduce the shared secret $s = P(0) \in \mathbb{Z}_{19}$. (4P)

7. *Cipolla.*

   (a) Show that 2 is a quadratic residue modulo 23.

   (b) Find the square roots of 2 modulo 23. Show first that $a = 0$ is a good choice such that $a^2 - 2$ is not a square modulo 23 and then compute in the field $\mathbb{F}_{23}[\sqrt{21}]$.

8. *Rings of remainders.* Solve the equation:

$$x^{256} = 1$$

   in the ring $(\mathbb{Z}/1024\,\mathbb{Z}, +, \times, 0, 1)$. How many solutions are there, and what is their form?

Every exercise gets 4 points.

For every modular inverse without computation, 1 point penalty.

For every exponentiation without computation, 1 point penalty.