Advanced Cryptography

November 24, 2021

1. *ADDITIVE Elgamal* modulo $n = 64$ with generator $g = 61$.
   (a) Alice chooses the secret key $x = 10$ while Bob chooses the temporary key $y = 11$. Compute the public key of Alice. Show how Bob encrypts the message $m = 12$ and how Alice decrypts the encrypted message.
   (b) Agent Eva computes $g^{-1} \bmod n$ and finds out the secret key of Alice using the public key of Alice. Make the computations.
2. *MULTIPLICATIVE Elgamal* modulo $p = 23$ in the group generated by $g = 2$. Alice has the public key $h = 18$. Bob sends the encrypted message $(c_1, c_2) = (9, 10)$. Decrypt the message.
3. *RSA*. Someone encrypted a message m modulo 85 using the public key $e = 11$ and got $c = 12$. Decrypt the message using the function $\lambda(N)$.
4. *Goldwasser-Micali.* Someone receives a message modulo 3521 consisting of the numbers 2899, 622, 1971, 1550. Decrypt the message.
5. *Shamir's No Key Protocol.* Alice sends to Bob the message $m = 10$ 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 $P \in \mathbb{Z}_{23}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{23} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{23}$. If three such pairs are $(1, 20)$, $(2, 16)$ and $(3, 10)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{23}$.
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. *RSA*. Let $p \neq q$ be two primes, $N = pq$, $\varphi = (p-1)(q-1)$ and $\lambda = \mathrm{lcm}(p-1, q-1)$. A RSA key is called a dead key if for all $m \in \mathbb{Z}_N$, $m^e = m \bmod N$. Let Δ be the set of dead keys in the interval $[1, \varphi]$.
   (a) Let $\cdot$ be the multiplication modulo φ. Show that $(\Delta, \cdot)$ is a group.
   (b) Show that $(a\lambda + 1)(b\lambda + 1) = ((a+b)\lambda + 1) \bmod \varphi$ for all $a, b \in \mathbb{Z}$.
   Conclude that $(\Delta, \cdot)$ is a cyclic group.
   (c) For $N = 85$, write down the group $(\Delta, \cdot)$ and verify that it is cyclic.

Every exercise gets 4 points.

For every modular inverse without computation, 1 point penalty.

For every exponentiation without computation, 1 point penalty.