Advanced Cryptography

September 5, 2021

1. *Additive Elgamal* modulo $n = 63$ with generator $g = 16$.
   (a) Alice chooses the secret key $x = 5$. Bob chooses the temporary key $y = 7$. Compute the public key of Alice. Show how Bob encrypts the message $m = 9$ and how Alice decrypts the encrypted message. (2P)
   (b) Agent Eve computes $g^{-1} \bmod n$ and deduces Alice's secret key from its public key. Make the computations. (2P)
2. *Multiplicative Elgamal* modulo $p = 19$ in the group generated by $g = 2$. Alice has the public key $h = 9$. Bob sends the encrypted message $(c_1, c_2) = (10, 11)$. Decrypt the message. (4P)
3. *RSA.* A message m modulo 91 is encrypted using the public key $e = 5$ and produces the cypher $c = 5$. Decrypt this cypher using the function $\mu(N)$. (4P)
4. *RSA.* Decrypt the cypher from Exercise 3 using the function $\lambda(N)$. (4P)
5. *Goldwasser-Micali.* An encrypted message modulo 77 consists of the numbers 23, 53, 36, 41. Decrypt the message. (4P)
6. *Shamir Secret Sharing.* Let $P \in \mathbb{Z}_{19}[X]$ be a polynomial of degree 2. Consider the following pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{19} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{19}$. If three pairs are $(1, 11)$, $(2, 13)$ and $(3, 16)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{19}$. (4P)
7. *Cipolla.*
   (a) Show that 7 is a quadratic remainder modulo 19. (1P)
   (b) Find the square roots of 7 modulo 19. To this goal, show that for $a = 1$, $a^2 - 7$ is not a quadratic remainder modulo 19 and make the computations in the field $\mathbb{F}_{19}[\sqrt{13}]$. (3P)
8. *Rings.* A commutative ring has exactly 3 elements which have multiplicative inverses. The number of the elements which have no multiplicative inverses is strictly smaller than 5. Show that this ring is the field with 4 elements, usually called $\mathbb{F}_4$. *Hints: What order has the element -1 in the multiplicative group of all invertible elements? Why does this imply that $1 = -1$? Use now the fact that a ring with $2 = 0$ is always a vector space over the field $\mathbb{F}_2$. It is known that such a finite vector field has a number of elements equal with a power of* 2. (4P)

Modular inverse without computation: 1 point penalty.

Modular exponential without computation: 1 point penalty.