Advanced Cryptography Exam

January 23, 2021

1. *ADDITIVE Elgamal* modulo $n = 256$ with generator $g = 127$.
   (a) Alice chooses the secret key $x = 129$ while Bob chooses the temporary key $y = 131$. Compute the public key of Alice. Show how Bob encrypts the message $m = 133$ and how Alice decrypts the encrypted message. (3P)
   (b) Agent Eva computes $g^{-1} \bmod n$ and finds out the secret key of Alice using the public key of Alice. Show how she does this. (1P)
2. *Multiplicative Elgamal* modulo $p = 23$ in the group generated by $g = 2$. Alice has the public key $h = 3$. Bob sends the encrypted message $(c_1, c_2) = (4, 5)$. Decrypt the message. (4P)
3. *RSA.* Someone encrypted a message m modulo 85 using the public key $e = 9$ and got $c = 10$. Decrypt the message using the function $\varphi(N)$. (4P)
4. *RSA.* Decrypt the message from Exercise 3 using the function $\lambda(N)$. (4P)
5. *Goldwasser-Micali Algorithm.* Someone receives a message modulo 2021 consisting of the numbers 269, 673, 1415, 1743. Decrypt the message. Use the fact that $2021 = 43 \cdot 47$. (4P)
6. *Shamir 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 $(5, 3)$, $(10, 15)$ and $(22, 10)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{23}$. (4P)
7. *Cipolla Algorithm.*
   (a) Show that 18 is a quadratic residue modulo 23. (1P)
   (b) Find the square roots of 18 modulo 23. Show first that $a = 3$ is a good choice such that $a^2 - 18$ is not a square modulo 23 and then compute in the field $\mathbb{F}_{23}[\sqrt{14}]$. (3P)
8. *RSA.* We know that in every commutative field $\mathbb{F}$, if a polynomial $f \in \mathbb{F}[X] \setminus \{0\}$ has degree d then f has at most d roots in $\mathbb{F}$. But the ring $\mathbb{Z}_N = \mathbb{Z}_{85}$ is not a field because $N = 85$ is not a prime number.

   Prove or disprove the following sentence:

   There is an $f \in \mathbb{Z}_{85}[X] \setminus \{0\}$ of degree $d = 17$ such that f has at least 18 roots in $\mathbb{Z}_{85}$.

   (4P)

Every exercise gets 4 points.

For every modular inverse without computation, 1 point penalty.

For every exponentiation without computation, 1 point penalty.