Advanced Cryptography

September 7, 2022

1. *ADDITIVE Elgamal* modulo $n = 100$ with generator $g = 33$.
   (a) Alice has the secret key $x = 5$. Bob has the temporary key $y = 6$. Compute the public key of Alice. Show how does Bob encrypt $m = 7$ and how does Alice decrypt the cypher. (2P)
   (b) Agent Eve computes $g^{-1} \bmod n$ and finds the secret key of Alice from its public key. Show how does this work in the given case. (2P)
2. *MULTIPLICATIVE Elgamal* modulo $p = 19$ in the group generated by $g = 2$. Alice has the public key $h = 13$. Bob sends the encrypted message $(c_1, c_2) = (15, 17)$. Decrypt the message. (4P)
3. *RSA.* A message m modulo 91 is encrypted with the public key $e = 7$. The result is $c = 10$. Decrypt the message using the function $\lambda(N)$. (4P)
4. *Goldwasser-Micali.* A message encrypted modulo 133 reads 95, 106, 38, 27. 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 $a = 3$ and Bob's secret key is $b = 11$. 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 $P(\alpha) \in \mathbb{Z}_{19}$: $(1, 9)$, $(2, 2)$ si $(3, 1)$. 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. *Permutations.* The six letters of a word are written on six cards. The cards are shuffled and put in a line from left to right. According to their order from left to right, they are called card 0, card 1, ..., card 5. For $0 \leq i < j \leq 5$, we call *operation* the following action: the card i is put on position j and the card j is put on position i.
   (a) Find the minimal number n such that the following proposition is true: *One needs at most n operations to restore the word.*
   (b) Let n be the answer to the question above. Show that there are permutations of the letters which can be solved by $n - 1$ operations but cannot be solved by n operations.

Every exercise gets 4 points.

For every modular inverse without computation, 1 point penalty.

For every exponentiation without computation, 1 point penalty.