Advanced Cryptography

June 7, 2023

1. *RSA* A message is encrypted using RSA modulo 91 with public key $e = 5$. The encrypted message is $c = 3$. Find the original message.

2. *Additive Elgamal* modulo $n = 100$ with generator $g = 11$. The public key is $h = 12$ and the encrypted message is $(c_1, c_2) = (13, 14)$. Find the clear message m.

3. *Multiplicative Elgamal* modulo $p = 19$ in the group generated by $g = 2$. The public key is $h = 6$, the encrypted message is $(c_1, c_2) = (3, 4)$. Find the clear message m.

4. *Shamir Secret Sharing.* Let $P \in \mathbb{Z}_{19}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{19} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{19}$. If 3 such pairs are $(10, 16)$, $(11, 0)$ and $(12, 5)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{19}$.

5. *Secret Multiparty Computation.* Alice, Bob and Cathy have secret values $x = 3$, $y = 3$ and $z = 3$ respectively. They want to compute together the value $z(x + y)$ in a way they trust, but without displaying the clear values of x, y and z. For sharing initial values, they use the polynomials $X + 3$, $2X + 3$ and $3X + 3$ respectively. For multiplication shares, they use polynomials of the shape $3X + a$, $X + b$ and $2X + c$ respectively. Run the whole protocol.

6. *Modular Arithmetic* Find an injective homomorphism (embedding) of the group $(\mathbb{Z}_{11}, +, 0)$ into the group $(\mathbb{Z}_{23} \setminus \{0\}, \cdot, 1)$. To achieve this goal, find an element $x \in \mathbb{Z}_{23}$ such that $x^2 \neq 1 \bmod 23$. What is the multiplicative order of x^2 in $\mathbb{Z}_{23}$?

Every exercise gets 1.5 points. One point is granted.

For every modular inverse without computation, 0.375 points penalty.

For every exponentiation without computation, 0.375 points penalty.

A correct answer without proof for exercise 6 gets only 0.375 points.