Advanced Cryptography

November 23, 2022

1. *RSA* A message is encrypted using RSA modulo 33 with public key $e = 13$. The encrypted message is $c = 20$. Find the original message.

2. *Additive Elgamal* modulo $n = 1000$ with generator $g = 143$. The public key is $h = 3$ and the encrypted message is $(c_1, c_2) = (2, 100)$. Find the clear message m.

3. *Multiplicative Elgamal* modulo $p = 29$ in the group generated by $g = 2$. The public key is $h = 19$, the encrypted message is $(c_1, c_2) = (7, 21)$. Find the clear message m.

4. *Shamir Secret Sharing.* Let $P \in \mathbb{Z}_{29}[X]$ be a polynomial of degree 2. Consider pairs $(\alpha, P(\alpha))$ where $\alpha \in \mathbb{Z}_{29} \setminus \{0\}$ and $P(\alpha) \in \mathbb{Z}_{29}$. If 3 such pairs are $(2, 11)$, $(4, 27)$ and $(8, 25)$, deduce the shared secret $s = P(0) \in \mathbb{Z}_{29}$.

5. *Secret Multiparty Computation.* Alice, Bob and Cathy have secret values $x = 1$, $y = 2$ and $z = 3$ respectively. They want to compute together the value $xz + yz$ in a way they trust, but without displaying the clear values of x, y and z. For sharing initial values, they use polynomials of the shape $X + a$, $2X + b$ and $3X + c$ respectively. For multiplication shares, they use polynomials of the shape $2X + a$, $3X + b$ and $X + c$ respectively. Run the whole protocol.

6. *Modular Arithmetic* How many solutions has the following equation:

   $$x^{64} = 1 \bmod 256$$

   in the ring of remainders $\mathbb{Z}_{256}$? Prove your answer.

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.