The ElGamal Cryptosystem

Ryan C. Daileda

Trinity University

Number Theory

Introduction

The next cryptosystem we will consider was created in 1985 and makes use of primitive roots.

The security of the system rests in the difficulty in solving the discrete logarithm problem $r^x \equiv a \pmod{p}$ or $x = \text{ind}_r(a)$.

As we have seen, as a function of a, $\text{ind}_r(a)$ appears to be essentially random, so it is a good choice for a basis of security.

ElGamal Keys

Every user of the ElGamal cryptosystem:

- Chooses a (large) prime p and one of its primitive roots r.
- Chooses a (secret) decryption key $K_D = k$ with $2 \leq k \leq p-2$ and computes

$$a \equiv r^k \pmod{p}, \quad 0 \leq a \leq p-1.$$

- Publishes the encryption key $K_E = (p, r, a)$.

Note that in order for an unauthorized party to determine $K_D = k$, they would need to compute $\text{ind}_r(a)$, which is a very hard problem.

ElGamal Encryption

To send a message to the user with public key $K_E = (p, r, a)$ the sender:

- Converts her message M into numerical blocks B of size $\leq p - 1$.
- Selects a (secret) j with $2 \leq j \leq p - 2$ and computes

  $$C_1 \equiv r^j \pmod{p} \quad \text{and} \quad C_2 \equiv Ba^j \pmod{p}, \quad 0 \leq C_1, C_2 \leq p-1$$

  for each block B. The key j can be changed with each block, if necessary.
- Sends the pairs (C_1, C_2).

ElGamal Decryption

The message block has been encrypted through multiplication by a^j, and the exponent j has been hidden in C_1.

Even though $K_E = (p, r, a)$ is public knowledge, extraction of j from C_1 requires the (difficult) computation of $\text{ind}_r(C_1)$.

But with the knowledge of $K_D = k$ the intended recipient can extract B (without knowing j) by computing

$$\begin{aligned} C_2 C_1^{p-1-k} &\equiv (Ba^j)(r^j)^{p-1-k} \pmod{p} \\ &\equiv B(r^k)^j r^{j(p-1)-jk} \pmod{p} \\ &\equiv B(r^{p-1})^j \equiv B \pmod{p}, \end{aligned}$$

where we have applied Fermat's Little Theorem in the final line.

Examples

Example 1

Encrypt the message RUN AWAY us the ElGamal key $(3137, 2894, 1505)$.

Solution. First we convert our message to base 27:

$$\begin{aligned} M =& 25 \cdot 27^7 + 1 \cdot 27^6 + 23 \cdot 27^5 + 1 \cdot 27^4 \\ &+ 0 \cdot 27^3 + 14 \cdot 27^2 + 21 \cdot 27 + 18 \\ =& 262226817657. \end{aligned}$$

We then parse the message into blocks of 3 digits:

$$B_1 = 657, B_2 = 817, B_3 = 226, B_4 = 262.$$

We choose the exponent $j = 2244$ and compute

$$\begin{aligned}
C_1 &\equiv r^j \equiv 2894^{2244} \equiv 2347 \pmod{3137},\\
C_{12} &\equiv B_1 a^j \equiv 657 \cdot 1505^{2244} \equiv 811 \pmod{3137},\\
C_{22} &\equiv B_2 a^j \equiv 817 \cdot 1505^{2244} \equiv 1973 \pmod{3137},\\
C_{32} &\equiv B_3 a^j \equiv 226 \cdot 1505^{2244} \equiv 2504 \pmod{3137},\\
C_{42} &\equiv B_4 a^j \equiv 262 \cdot 1505^{2244} \equiv 99 \pmod{3137}.
\end{aligned}$$

Finally we transmit the pairs

$$\boxed{(2347, 811),\ \ (2347, 1973),\ \ (2347, 2504),\ \ (2347, 99)}.$$

Example 2

The message pairs $(1748, 770)$, $(2572, 1908)$, $(1116, 198)$, $(798, 2270)$, $(766, 2073)$ were encrypted using the ElGamal encryption key of the preceding example. Use the fact that the decryption key is $K_D = 2147$ to decrypt the message.

Solution. Apparently a different j was used to encrypt each block, but the decryption process is nonetheless the same.

For each pair (C_1, C_2) we compute

$$C_2 C_1^{p-1-k} \equiv C_2 C_1^{989} \pmod{3137}.$$

This yields

$$\begin{aligned} 770 \cdot 1748^{989} &\equiv 970 \pmod{3137}, \\ 1908 \cdot 2572^{989} &\equiv 132 \pmod{3137}, \\ 198 \cdot 1116^{989} &\equiv 513 \pmod{3137}, \\ 2270 \cdot 798^{989} &\equiv 627 \pmod{3137}, \\ 2073 \cdot 766^{989} &\equiv 99 \pmod{3137}. \end{aligned}$$

Concatenating yields the complete message

$$M = 99627513132970.$$

Repeatedly dividing by 27 yields the base 27 "digits"

$$13, 1, 20, 8, 0, 18, 15, 3, 11, 19,$$

which translate to MATH ROCKS. □

Digital Signatures

Given that the encryption keys of a public key cryptosystem are not secret, it is important to be able to authenticate the sender of any message.

Any member of an ElGamal cryptosystem can use their own public and private keys to append a *digital signature* to any message.

The message sender choses an exponent j and computes $c \equiv r^j \pmod{p}$ using their own public key $K_E = (p, r, a)$.

The sender then takes the first plaintext block B and uses the EA to solve the linear congruence

$$jd + kc \equiv B \pmod{p-1},$$

where $K_D = k$ is the sender's secret decryption key.

The sender then appends the digital signature (c, d) to the encrypted message.

Note that in order to have computed (c, d) the sender must be in possession of k, j and B, all of which are secret.

To check the signature the recipient of the message decrypts the first plaintext block B and then uses the sender's key $K_E = (p, r, a)$ to compute

$$V_1 \equiv a^c c^d \pmod{p} \quad \text{and} \quad V_2 \equiv r^B \pmod{p}.$$

The signature is valid as long as $V_1 = V_2$, since

$$V_1 \equiv a^c c^d \equiv (r^k)^c (r^j)^d \equiv r^{kc+jd} \equiv r^B \equiv V_2 \pmod{p}.$$