The ElGamal Cryptosystem

Justin Wyss-Gallifent

March 8, 2022

0.1 Introduction

The ElGamal cryptosystem is based on the fact that it is easy to raise things to powers in modular arithmetic but difficult to take (discrete) logarithms.

0.2 Key Creation

Bob selects a prime p, a primitive root α of p, and an integer a with $0 \leq a \leq p-1$. The value a is kept private.

Bob then calculates the least nonnegative residue $\beta \equiv \alpha^a \mod p$. The triple (p, α, β) is then made public.

Observe that $a \equiv \text{ind}_r \beta \mod p-1$ and this is difficult to calculate.

0.3 Encryption

Suppose Alice wants to send a plaintext block $0 \leq P < p$ to Bob. She first chooses a random number $1 \leq k \leq p-2$. Then she encrypts via the encryption function by:

$$\mathcal{E}(P) \equiv (\alpha^k, P\beta^k) \mod p$$

This produces a pair (γ, δ) which constitutes the cipertext. That is, $\gamma \equiv \alpha^k \mod p$ and $\delta = P\beta^k \mod p$.

Typically a different k is used for each plaintext block. The primary reason for this is that then identical plaintext blocks will have different corresponding ciphertext blocks.

0.4 Decryption

To decrypt the ciphertext block (γ, δ) we claim that;

$$P \equiv \gamma^{p-1-a}\delta \mod p$$

This works because of the following, where the negative exponent means the multiplicative inverse.

$$\begin{aligned}
\gamma^{p-1-a}\delta &= (\alpha^k)^{p-1-a} P\beta^k \mod p \\
&= (\alpha^{p-1})^k (\alpha^a)^{-k} \beta^k P \mod p \\
&= (1)^k \beta^{-k} \beta^k P \mod p \\
&= P \mod p
\end{aligned}$$

Thus we have the decription function:

$$\mathcal{E}^{-1}(\gamma, \delta) \equiv \gamma^{p-1-a}\delta \mod p$$

0.5 Encryption/Decryption Example

Bob selects $p = 2539$, $\alpha = 2$ (this is a primitive root), and $a = 42$. He keeps $a = 42$ private. He calculates $\beta \equiv 2^{42} \equiv 1305 \mod 2539$ and makes $(p, \alpha, \beta) = (2539, 2, 1305)$ public.

Alice wants to send him `OHNO` so she splits it as `OH`=1407 and `NO`=1314.

- To encrypt 1407 she chooses $k = 100$ and calculates:

$$\mathcal{E}(1407) \equiv (2^{100}, 1407 \cdot 1305^{100}) \equiv (613, 635) \mod 2539$$

- To encrypt 1314 she chooses $k = 200$ and calculates:

$$\mathcal{E}(1314) \equiv (2^{200}, 1314 \cdot 1305^{200}) \equiv (2536, 1404) \mod 2539$$

She sends these two pairs to Bob.

Bob receives them and decrypts via:

- To decrypt $(613, 635)$ he does:

$$\mathcal{E}^{-1}(613, 635) \equiv 613^{2539-1-42} 635 \equiv 1407 \mod 2539$$

- To decrypt $(2536, 1404)$ he does:

$$\mathcal{E}^{-1}(2536, 1404) \equiv 2536^{2539-1-42} 1404 \equiv 1314 \mod 2539$$

0.6 Signatures

Let's see how Alice can sign a message. Suppose Alice has the public key (p, α, β) and the private key a and wishes to sign the message $0 \leq m < p$. She chooses $1 \leq k \leq p-2$ with $\gcd(k, p-1) = 1$ and computes:

$$r \equiv \alpha^k \mod p$$
$$s \equiv k^{-1}(m - ra) \mod p - 1$$

Note here that k^{-1} is the mod $p-1$ inverse which exists because $\gcd(k, p-1) = 1$.

Note also the fact that Alice uses her own private a for this.

The signed message which she sends is then (m, r, s). Notice that the message m is included in plaintext. There is nothing hidden here!

To verify that (m, r, s) came from Alice, Bob checks whether:

$$\beta^r r^s \equiv \alpha^m \mod p$$

If this is true, the signature is considered valid.

First let's check that for a valid message this will be true. Observe that $ks \equiv m - ar \mod p-1$ and so $m \equiv ks + ar \mod p-1$ and then:

$$\alpha^m \equiv \alpha^{sk+ar} \equiv (\alpha^a)^r \left(\alpha^k\right)^s \equiv \beta^r r^s \mod p$$

Second we should understand why this is hard to fake. Why is it difficult for Eve to take her own m and construct r and s with $\beta^r r^s \equiv \alpha^m \mod p$? Well, consider that she can certainly pick a $1 \leq k \leq p-2$ with $\gcd(k, p-1) = 1$ and since α is public she can calculate $r \equiv \alpha^k \mod p$. At this point she needs some s with $\beta^r r^s \equiv \alpha^m \mod p$, but this means solving a discrete logarithm problem, and this is thought to be hard.

0.7 Signing/Verification Example

Suppose Alice has chosen the prime $p = 253679$ and the primitive root $\alpha = 17$. She then chooses $a = 2468$ and calculates $\beta \equiv \alpha^a \equiv 202478 \mod p$. Her public key is then $(p, \alpha, \beta) = (253679, 17, 202478)$ and her private key is $a = 2468$.

Suppose she wishes to sign the message `ZIP`, which converts to 250815.

She chooses $k = 12345$, noting that $\gcd(12345, 253678) = 1$, and calculate the $k^{-1} \equiv 14035 \mod 253678$. She then calculates:

$$r \equiv \alpha^k \equiv 17^{12345} \equiv 9945 \mod 253679$$
$$s \equiv k^{-1}(m - ra) \equiv 14035(250815 - 9945 \cdot 2468) \equiv 205783 \mod 253678$$

She sends:

$$(m, r, s) = (250815, 9945, 205783)$$

Bob receives $(m, r, s) = (250815, 9945, 205783)$ and verifies it:

$$\beta^r r^s \equiv 202478^{9945} 9945^{205783} \equiv 43257 \mod 253679$$
$$\alpha^m \equiv 17^{250815} \equiv 43257 \mod 253679$$

0.8 Signing Note

It is very important that Alice does not use the same k to sign two different messages. Let's see why. This example is taken from Trappe/Washington, I've just rewritten it in what I think is a more clear form. Also there is a typo in the book.

Suppose Alice has chosen the prime $p = 225119$ and the primitive root $\alpha = 11$. She then chooses her secret a which we won't give for now and she calculates $\beta \equiv \alpha^a \equiv 18191 \mod 225119$. Now she signs two messages but uses the same k, which we also won't give for now!

- She signs $m_1 = 151405$ with k:

$$r_1 \equiv \alpha^k \equiv 11^k \equiv 164130 \mod 225119$$
$$s_1 \equiv k^{-1}(m_1 - ar_1) \equiv 130777 \mod 225118$$

  This yields $(m_1, r_1, s_1) = (151405, 164130, 130777)$.

- She signs $m_2 = 202315$ with k:

$$r_2 \equiv \alpha^k \equiv 11^k \equiv 164130 \mod 225119$$
$$s_2 \equiv k^{-1}(m_2 - ar_2) \equiv 164899 \mod 225118$$

  This yields $(m_2, r_2, s_2) = (202315, 164130, 130777)$.

Immediately Eve sees that $r_1 = r_2$ since they're both 11^k for the same k and so she knows that the k are identical since α is a primitive root.

Eve knows that:

$$s_1 \equiv k^{-1}(m_1 - ar_1) \mod p - 1$$
$$s_2 \equiv k^{-1}(m_2 - ar_2) \mod p - 1$$

This is:

$$130777 \equiv k^{-1}(151405 - 164130a) \mod 225118$$
$$164899 \equiv k^{-1}(202315 - 164130a) \mod 225118$$

She rewrites this as:

$$130777k \equiv 151405 - 164130a \mod 225118$$
$$164899k \equiv 202315 - 164130a \mod 225118$$

Subtracting yields:

$$190996k \equiv 174208 \mod 225118$$

Since $\gcd(190996, 225118) = 2 \mid 174208$ there are two solutions for k which are $k = 239$ and $k = 112798$.

She checks which of these satisfies $r_1 \equiv \alpha^k \mod p$:

$$\alpha^{239} \equiv 11^{239} \equiv 164130 \mod 225119$$
$$\alpha^{112798} \equiv 11^{112798} \equiv 60989 \mod 225119$$

Since the first works, she knows $k = 239$.

She then writes the equation:

$$130777(239) \equiv 151405 - 164130a \mod 225118$$
$$164130a \equiv 187104 \mod 225118$$

Since $\gcd(164130, 225118) = 2 \mid 187104$ there are two solutions for a which are $a = 28862$ and $a = 141421$.

She checks which of these satisfes $\alpha^a \equiv \beta \mod p$:

$$11^{28862} \equiv 206928 \mod 225119$$
$$11^{141421} \equiv 18191 \mod 225119$$

Since the second works, she knows $a = 141421$.

0.9 Notes

1. To decrypt a message Eve needs to know a which as we have said involves taking the discrete logarithm of β using the primitive root α.
2. Although r is known and arguably one could try lots of a until $\alpha^a \equiv \beta \mod p$, in practice if p is large this is impractical.
3. Because each plaintext block gets its own choice of k, identical plaintext blocks will have different ciphertext blocks.
4. The ciphertext is twice as long as the plaintext. The advantage is that noted above.
5. As with most cryptosystems (we didn't mention this with RSA) in practice this would be used to share symmetric key which is then used to encrypt and decrypt the message.
6. While it's possible to sign messages using ElGamal, the method is not quite as simple as with RSA. With RSA Alice would simply user her own decryption key but here decryption works on pairs (γ, δ) which emerge from (P, k) and not on single blocks of text.
7. Verifying primitive roots can take a while but since Bob's p and α are public it doesn't matter how he obtains them or who knows. Heck, Alice could have given them to him. It's the a that's critical.
8. Alice should definitely choose a random k each time. If she encrypts both P_1 and P_2 with the same k and if Eve figures out P_1 then she can figure out P_2. This is because $\delta_1 \equiv P_1 b^k \mod p$ and $\delta_2 \equiv P_2 b^k \mod p$ and since Eve knows δ_1 and δ_2 she can calculate:

$$P_2 \equiv \delta_2 (\beta^k)^{-1} \equiv \delta_2 (\delta_1 P_1^{-1})^{-1} \equiv \delta_2 \delta_1^{-1} P_1 \mod p$$

9. It may not be clear what the relevance of r being a primitive root is. The reason we want a primitive root is that this guarantees that there is only one $0 \leq a \leq p-1$ such that $\alpha^a \equiv b \mod p$. If α is not a primitive root then there will be more than one a, potentially many, which makes it much easier to obtain an a which works, either by brute force or by more sophisticated methods.
10. ElGamal does not have perfect secrecy.