Review. ElGamal encryption

Example 150. Does Alice have to choose a new y if she sends several messags to Bob using ElGamal encryption?

Solution. Yes, she absolutely has to randomly choose a new y every time! Here's why:

If she was using the same y to encrypt messages $m^{(1)}$ and $m^{(2)}$, Alice would be sending the ciphertexts $(c_1^{(1)}, c_2^{(1)}) = (g^y, g^{xy}m^{(1)})$ and $(c_1^{(2)}, c_2^{(2)}) = (g^y, g^{xy}m^{(2)})$.

That means, Eve can immediately figure out $c_2^{(1)} / c_2^{(2)} = m^{(1)} / m^{(2)}$ (the divison is a modular inverse and everything is modulo p). That's a combination of the plaintexts, and Eve should never be able to get her hands on such a thing.

(Note that Eve would know right away if Alice is doing the mistake of reusing y because $c_1^{(1)} = c_1^{(2)}$.)

Comment. The situation is just like for the one-time pad (in that case, reusing the key reveals $m^{(1)} \oplus m^{(2)}$).

The computational and decisional Diffie–Hellman problem

We indicated that the security of ElGamal depends on the difficulty of computing discrete logarithms. Here is a more precise statement.

Theorem 151. Decrypting c to m in ElGamal is exactly as difficult as the **computational Diffie–Hellman problem** (CDH).

The CDH problem is the following: given $g, g^x, g^y \pmod{p}$, find $g^{xy} \pmod{p}$. It is believed to be hard.

Proof. Recall that the public key is $(p, g, h) = (p, g, g^x)$. The ciphertext is $c = (g^y, h^y m) = (g^y, g^{xy} m)$.
Hence, determining m is equivalent to finding g^{xy}.
Since $g, g^x, g^y \pmod{p}$ are known, this is precisely the CDH problem. □

Example 152. In fact, even the **decisional Diffie–Hellman problem** (DDH) is believed to be difficult.

The DDH problem is the following: given $g, g^x, g^y, r \pmod{p}$, decide whether $r \equiv g^{xy} \pmod{p}$. Obviously, this is simpler than the CDH problem, where g^{xy} needs to be computed. Yet, it, too, is believed to be hard.

Comment. Well, at least it is hard (modulo p) if we always want to do better than guessing.

Here's how we can sometimes do better than guessing: if g^x or g^y are quadratic residues (this is actually easy to check modulo primes p using quadratic reciprocity and the Legendre symbol), then g^{xy} is a quadratic residue (why?!). Hence, if r is not a quadratic residue, we can conclude that $r \not\equiv g^{xy}$.

Comments on primitive roots

Our next goal is to observe the following:

There are $\phi(\phi(p)) = \phi(p-1)$ primitive roots modulo a prime p.

Why? First of all, one can show that there do exist primitive roots modulo primes. The claimed number of these primitive roots then follows from Example 154. First, we start with a warm-up example though.

Example 153. If Bob selects $p = 23$ for ElGamal, how many possible choices does he have for g? Which are these?

Solution. In short, Bob has $\phi(p-1) = \phi(22) = 10$ choices for g. Let's go through the details:
g must be a primitive root modulo p.

- Here, the smallest primitive root is $g = 5$. [Modulo a prime p, there always exists a primitive root g.]
  To check that, we need to verify that the order of $5 \pmod{23}$ is 22. Since the order must divide 22, it is enough to check that $5^2 \not\equiv 1 \pmod{23}$ and $5^{11} \not\equiv 1 \pmod{23}$.
- By definition, g has order $p-1$. Then, all other invertible residues can be expressed as g^a, which has order $(p-1)/\gcd(p-1, a)$. In order for g^a to be a primitive root, we therefore need $\gcd(p-1, a) = 1$. There are $\phi(p-1) = \phi(22) = 10$ such values a in the range $1, 2, \ldots, 22$.
- The possible 10 values for a are $1, 3, 5, 7, 9, 13, 15, 17, 19, 21$.
  The corresponding 10 primitive roots are $5^1, 5^3, 5^5, 5^7, \ldots \pmod{23}$. Explicitly computing these powers, the primitive roots are $5, 7, 10, 11, 14, 15, 17, 19, 20, 21 \pmod{23}$.

Proceeding as in the previous example, we obtain the following result.

Theorem 154. (number of primitive roots) Suppose there is a primitive root modulo n. Then there are $\phi(\phi(n))$ primitive roots modulo n.

Proof. Let x be a primitive root. It has order $\phi(n)$. All other invertible residues are of the form x^a.
Recall that x^a has order $\frac{\phi(n)}{\gcd(\phi(n), a)}$. This is $\phi(n)$ if and only if $\gcd(\phi(n), a) = 1$. There are $\phi(\phi(n))$ values a among $1, 2, \ldots, \phi(n)$, which are coprime to $\phi(n)$.
In conclusion, there are $\phi(\phi(n))$ primitive roots modulo n. □

Comment. Recall that, for instance, there is no primitive root modulo 15. That's why we needed the assumption that there should be a primitive root modulo n (which is the case if and only if n is of the form $1, 2, 4, p^k, 2p^k$ for some odd prime p).