## The ElGamal public key cryptosystem and discrete logarithms

Whereas the security of RSA relies on the difficulty of factoring, the security of ElGamal and Diffie–Hellman relies on the difficulty of computing discrete logarithms.

### Discrete logarithms

Suppose $b = a^x \pmod N$. Finding $x$ is called the **discrete logarithm problem** mod $N$. If $N$ is a large prime $p$, then this problem is believed to be difficult.

**Note.** If $b = a^x$, then $x = \log_a(b)$. Here, we are doing the same thing, but modulo $N$. That's why the problem is called the discrete logarithm problem.

**Example 166.** Find $x$ such that $4 \equiv 3^x \pmod 7$.

**Solution.** We have seen in Example 152 that $3$ is a primitive root modulo $7$. Hence, there must be such an $x$. Going through the possibilities ($3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 4$), we find $x = 4$, because $3^4 \equiv 4 \pmod 7$.

**Example 167.** Find $x$ such that $3 \equiv 2^x \pmod{101}$.

**Solution.** Let us check that the solution is $x = 69$. Indeed, a quick binary exponentiation confirms that $2^{69} \equiv 3 \pmod{101}$. (Do it!)

The point is that it is actually (believed to be) very difficult to compute these **discrete logarithms**. On the other hand, just like with factorization, it is super easy to verify the answer if somebody tells us the answer.

**Comment.** We can check that $2$ is a primitive root modulo $101$. That is, $2 \pmod{101}$ has (multiplicative) order $100$. That means every equation $2^x \equiv a \pmod{101}$, where $a \not\equiv 0$, has a solution.

### Diffie–Hellman key exchange

**(Diffie–Hellman key exchange)**

- Alice and Bob select a large prime $p$ and a primitive root $g \pmod p$.
- Bob randomly selects a secret integer $x$ and reveals $g^x \pmod p$ to everyone.
  Alice randomly selects a secret integer $y$ and reveals $g^y \pmod p$ to everyone.
- Alice and Bob now share the secret $g^{xy} \pmod p$.
  Indeed, Alice can compute $g^{xy} = (g^x)^y$ using the public $g^x$ and her secret $y$.
  Likewise, Bob can compute $g^{xy} = (g^y)^x$ using the public $g^y$ and his secret $x$.

**Why is this secure?** We need to see why eavesdropping Eve cannot (simply) obtain the secret $g^{xy} \pmod p$. She knows $g$, $g^x$, $g^y \pmod p$ and needs to find $g^{xy} \pmod p$. This is the **computational Diffie–Hellman problem** (CDH), which is believed to be hard (it would be easy if we could compute discrete logarithms).

**Example 168.** You are Eve. Alice and Bob select $p = 53$ and $g = 5$ for a Diffie–Hellman key exchange. Alice sends $43$ to Bob, and Bob sends $20$ to Alice. What is their shared secret?

**Solution.** If Alice's secret is $y$ and Bob's secret is $x$, then $5^y \equiv 43$ and $5^x \equiv 20 \pmod{53}$.

Since we haven't learned a better method, we just compute $5^2, 5^3, \ldots$ until we find $43$ or $20$:

$5^2 = 25$, $5^3 \equiv 19$, $5^4 \equiv 19 \cdot 5 \equiv -11$, $5^5 \equiv -11 \cdot 5 \equiv -2$, $5^6 \equiv -2 \cdot 5 \equiv -10 \equiv 43 \pmod{53}$.

Hence, Alice's secret is $y = 6$. The shared secret is $20^6 \equiv 9 \pmod{53}$.

**Note.** We don't need to find Bob's secret. [It is $x = 11$.]

Armin Straub
straub@southalabama.edu