Section 5 Lecture 33 - Diffie-Hellman key exchange

Diffie-Hellman key exchange was one of the first practical uses of public-key ideas. It is not a full public-key cryptography scheme, but rather a way to establish a shared secret key in order to then use a secret-key cipher.

As with all public-key ideas, it relies on a mathematical problem that is "easy" one way and "hard" the other way.

Diffie-Hellman key exchange

The essential principle of Diffie-Hellman key exchange is given below:

- Alice and Bob choose a prime p and a *base* g (g must be a *primitive root* (mod p))
- Alice chooses a secret integer a and sends $A = g^a \pmod{p}$ to Bob
- Bob chooses a secret integer b and sends $B = g^b \pmod{p}$ to Alice
- Bob calculates $A^b \pmod{p}$
- Alice calculates $B^a \pmod{p}$
- These values are equal (both are $g^{ab} \pmod{p}$) and used as the secret key

Example

Suppose Alice and Bob agree to use $p = 19$ and $g = 3$. Alice chooses secret integer 4 and Bob chooses secret integer 8.

- Alice calculates $A = g^a \pmod{p} = 3^4 \pmod{19} = 5$ and sends 5 to Bob.
- Bob calculates $B = g^b \pmod{p} = 3^8 \pmod{19} = 6$ and sends 6 to Alice.
- Bob calculates $A^b \pmod{p} = 5^8 \pmod{19} = 4$
- Alice calculates $B^a \pmod{p} = 6^4 \pmod{19} = 4$
- The shared secret key is agreed as 4

And that's all there is to it! Note that there is no connection between the answer 4 and the fact that Alice's secret key is 4 – that's just coincidence.

Security

This process is secure for large primes p. Even if someone intercepts the messages being sent ($g^a \pmod{p}$ and $g^b \pmod{p}$) they cannot, in any feasible time, calculate g and hence work out $g^{ab} \pmod{p}$. This is known as the *discrete logarithm problem*. Note that Bob and Alice each have their own secret key that they never share with anyone, not even the people they are communicating with.

It doesn't, as it stands, provide any *authentication* – anyone could pretend to be Alice or Bob and communicate. This can be resolved inside a *public-key infrastructure* – more to come on this later in the course!