

# Foundations of Computer Security

## Lecture 52: Diffie-Hellman Key Exchange

Dr. Bill Young

Department of Computer Sciences

University of Texas at Austin

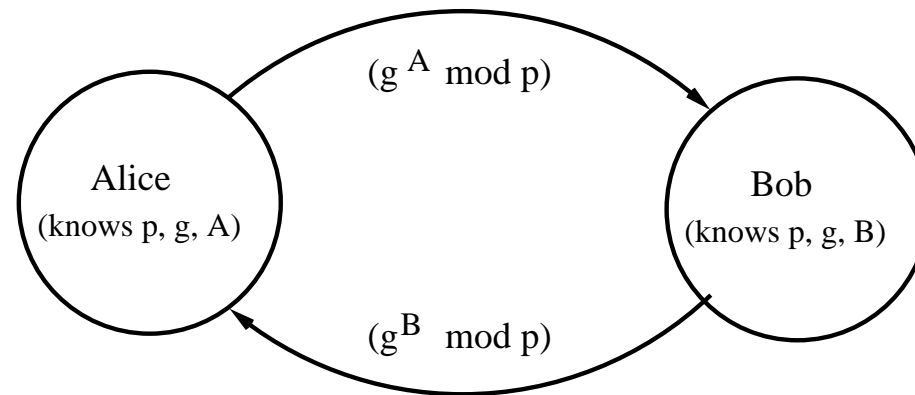
# Diffie-Hellman Key Exchange

The question of key exchange was one of the first problems addressed by a cryptographic protocol. *This was prior to the invention of public key cryptography.*

The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel.

The point is to agree on a key that two parties can use for a symmetric encryption, in such a way that an eavesdropper cannot obtain the key.

# Diffie-Hellman Algorithm



Steps in the algorithm:

- 1 Alice and Bob agree on a prime number  $p$  and a base  $g$ .
- 2 Alice chooses a secret number  $a$ , and sends Bob  $(g^a \text{ mod } p)$ .
- 3 Bob chooses a secret number  $b$ , and sends Alice  $(g^b \text{ mod } p)$ .
- 4 Alice computes  $((g^b \text{ mod } p)^a \text{ mod } p)$ .
- 5 Bob computes  $((g^a \text{ mod } p)^b \text{ mod } p)$ .

Both Alice and Bob can use this number as their key. Notice that  $p$  and  $g$  need not be protected.

# Diffie-Hellman Example

- 1 Alice and Bob agree on  $p = 23$  and  $g = 5$ .
- 2 Alice chooses  $a = 6$  and sends  $5^6 \bmod 23 = 8$ .
- 3 Bob chooses  $b = 15$  and sends  $5^{15} \bmod 23 = 19$ .
- 4 Alice computes  $19^6 \bmod 23 = 2$ .
- 5 Bob computes  $8^{15} \bmod 23 = 2$ .

Then 2 is the shared secret.

Clearly, much larger values of  $a$ ,  $b$ , and  $p$  are required. An eavesdropper cannot discover this value even if she knows  $p$  and  $g$  and can obtain each of the messages.

# Diffie-Hellman Security

Suppose  $p$  is a prime of around 300 digits, and  $a$  and  $b$  at least 100 digits each.

Discovering the shared secret given  $g$ ,  $p$ ,  $g^a \bmod p$  and  $g^b \bmod p$  would take longer than the lifetime of the universe, using the best known algorithm. This is called the *discrete logarithm problem*.

- How can two parties agree on a secret value when all of their messages might be overheard by an eavesdropper?
- The Diffie-Hellman algorithm accomplishes this, and is still widely used.
- With sufficiently large inputs, Diffie-Hellman is very secure.

**Next lecture:** Digital Signatures