Diffie-Hellman Key Exchange

MAT231

Transition to Higher Mathematics

Fall 2014

Outline

1. Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange

Consider the following problem:

- Two people (or computers) need to communicate securely.
- They have access to a *symmetric cypher* (the same key is used for encryption and decryption).
- They have not yet agreed on a key (they may not have ever met or communicated before).

The challenge here is "how can these two people decide on a key to use without anyone being able to capture it?"

Diffie-Hellman Key Exchange

Consider the following problem:

- Two people (or computers) need to communicate securely.
- They have access to a *symmetric cypher* (the same key is used for encryption and decryption).
- They have not yet agreed on a key (they may not have ever met or communicated before).

The challenge here is "how can these two people decide on a key to use without anyone being able to capture it?"

The first effective public key exchange method is known as **Diffie-Hellman Key Exchange** after the researchers that discovered it.

Diffie-Hellman Key Exchange

Because they were used in the original description of the algorithm, Diffie-Hellman key exchange is usually described assuming that Alice and Bob want to use a symmetric cipher and so need to exchange a private key.

1. Alice and Bob agree on two numbers g and p with $0 < g < p$. These numbers are not private and can be known by anyone.
2. Alice picks a private number $0 < a$ and computes $\alpha = g^a \bmod p$. Alice sends α to Bob.
3. Meanwhile, Bob picks a private number $0 < b$ and computes $\beta = g^b \bmod p$. He then sends β to Alice.
4. Alice computes $k = \beta^a \bmod p$ and Bob computes $k = \alpha^b \bmod p$. Both of them obtain the same number k which can then be used as the secret key.

Diffie-Hellman Key Exchange

Example: Alice and Bob agree on $g = 327$ and $p = 919$.

- Alice chooses $a = 400$; this is her *private key*. She then computes $\alpha = 327^{400} \bmod 919 = 231$. This is Alice's *public key* and can be known by anyone. She can send this number to Bob in cleartext.
- Bob chooses $b = 729$ for his *private key* and computes $\beta = 327^{729} \bmod 919 = 162$ and sends this number (his *public key*) to Alice.
- Alice computes $k = 162^{400} \bmod 919 = 206$.
- Bob computes $k = 231^{729} \bmod 919 = 206$.
- $k = 206$ is the secret key that both Alice and Bob will use to encrypt their messages to each other.

Fast Modular Exponentiation

Purpose: Compute $x^n \bmod m$ using fast modular arithmetic.

Usage: `r = fastexp( x, n, m )`

Input:
- `x` (unsigned integer) the base
- `n` (unsigned integer) the exponent
- `m` (unsigned integer) the modulus

Output:
- `r` (unsigned integer) $x^n \bmod m$

```
def fastexp( x, n, m ):
    x = x % m
    r = 1
    while n > 0:
        if n % 2 == 1:
            r = ( r * x ) % m
        x = ( x * x ) % m
        n = n / 2
    return r
```