Cryptography

Samuel Kim
May 7, 2015

The magic words are squeamish ossifrage.

1 Introduction

Cryptography is the study of secure communication. To this end, many cryptosystems have been developed. Many modern cryptosystems rely on number theory.

2 Diffie-Hellman Key Exchange

2.1 Description

Alice and Bob agree on a prime modulus p and an integer g, $1 < g < p$. They each choose a random integer (a and b), and send g to the power of that integer modulo p (A and B) to each other. To calculate the shared key, they raise the integer they receive to the power of their integer.

2.2 Attacks

2.2.1 Man-In-The-Middle

If Mallory is able to intercept the messages, she can initiate two different key exchanges, and decrypt and modify messages.

Countermeasure There are variants of Diffie-Hellman that use an asymmetric key pair to digitally sign messages, ensuring that they are not modified in transit.

2.2.2 Pollig-Hellman Algorithm

Problem: Given that $g^x \equiv e \pmod{p}$, find x.

Algorithm 1 Pollig-Hellman Algorithm

```
1: function PolligHellman(p,g,e)
2:     P ← prime factorization of p − 1
3:     B ← new int[P.length]
4:     for i = 0; i < P.length; i++ do
5:         B[i] ← b_i, where x ≡ b_i (mod p_i^{e_i})
6:     end for
7:     x ← CRT(B,P)
8:     return x
9: end function
```

Worst case time-complexity: $O(\sqrt{n})$, as the largest prime factor $\leq \sqrt{n}$.

Countermeasure The order of the group (in this case, $p-1$) should have large factors. We can choose a *safe prime*, where $p = 2q - 1$, for q prime.

3 RSA

3.1 Description

Alice calculates two large primes, p and q, and computes $n = pq$. She then picks a *public exponent* e relatively prime to $\varphi(n)$, and calculates the *private exponent* d by finding the inverse of e modulo $\varphi(n) = (p-1)(q-1)$. She sends her public key (n, e) to Bob. If Bob wants to send a message to Alice, he turns the message into an integer m, and sends $c = m^e \pmod{n}$ to Alice. Alice then decrypts c by raising it to the power of her private exponent d modulo n.

3.2 Attacks

3.2.1 Low Public Exponent

If e and m are sufficiently small enough, $m^e < n$, so c can simply be decrypted by finding the e^{th} root.

Håstad's Broadcast Attack If m is transmitted to at least e people with the same public exponent e, then we can use CRT to find $m^e \pmod{n_1 n_2 \cdots n_e}$. Since $m < n_i$, $m^e < n_1 n_2 \cdots n_e$, and we can take the e^{th} root. There is a stronger version of this attack that works even when the message is linearly padded.

Countermeasure To prevent this, there are various schemes for padding the message with random data. In addition, the public exponent should be large ($2^{16} + 1 = 65537$ in practice).

3.2.2 Low Private Exponent

Wiener's Attack If $d < \frac{1}{3} n^{1/4}$ and $q < p < 2q$, d can be efficiently recovered.

Countermeasure The private exponent should be calculated from the chosen public exponent.

4 Elliptic Curves

An elliptic curve (for our purposes) is a curve of the equation $y^3 = x^3 + ax + b$. If we add a "point at infinity," and set the condition that 3 points on a line (counting a point twice if tangent) sum to the point at infinity, we get an abelian (commutative) group, with the point at infinity being the identity element, and addition being the operation.

Since precision is an issue with real numbers, we instead look at elliptic curves over integers modulo some prime p.

4.1 Elliptic Curve Discrete Log

Given a point A on an elliptic curve and a positive integer n, we can compute nA efficiently by repeated doubling. In addition, given nA and A, it's hard to find n without resorting to brute-force. Thus, we can use elliptic curves in algorithms that rely on the discrete log problem, like Diffie-Hellman.

4.2 Attacks

Some curves are weak, and make the discrete log problem easier to crack. For example, certain curves over $\mathbb{F}_p$ are *anomalous*, with only p points.