Cryptography

Algorithms and Attacks

Samuel Kim
September 17, 2014

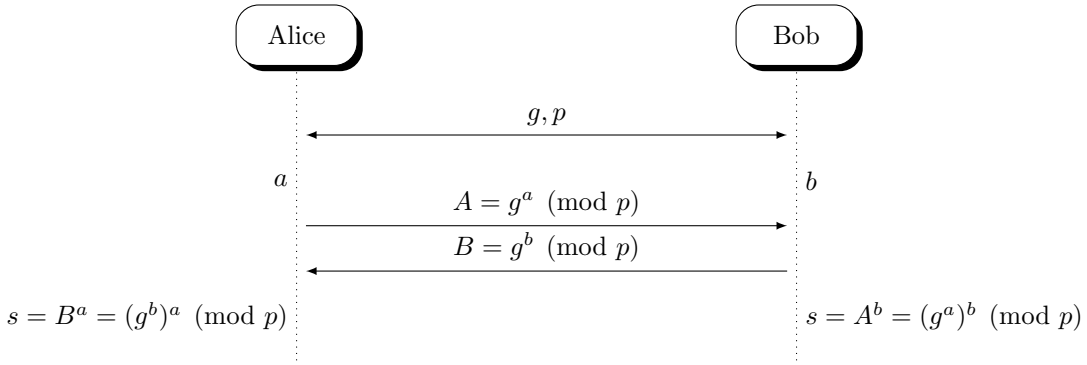
The magic words are squeamish ossifrage.

1 Introduction

Many cryptosystems rely on number theory, and the difficulty of solving certain problems, such as the discrete-log problem and the problem of factoring large integers efficiently. Here's a small sampler of algorithms in cryptography that use number theory.

2 Diffie-Hellman Key Exchange

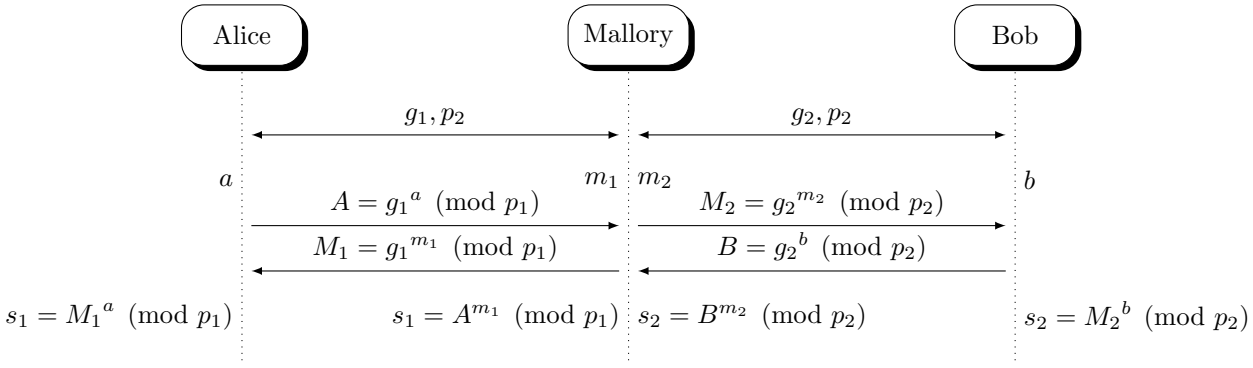
2.1 Description



Alice and Bob agree on a prime modulus p and an integer $g \in (\mathbb{Z}/p\mathbb{Z})^\times$, preferably with an order of a multiple of a large prime (for security). 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

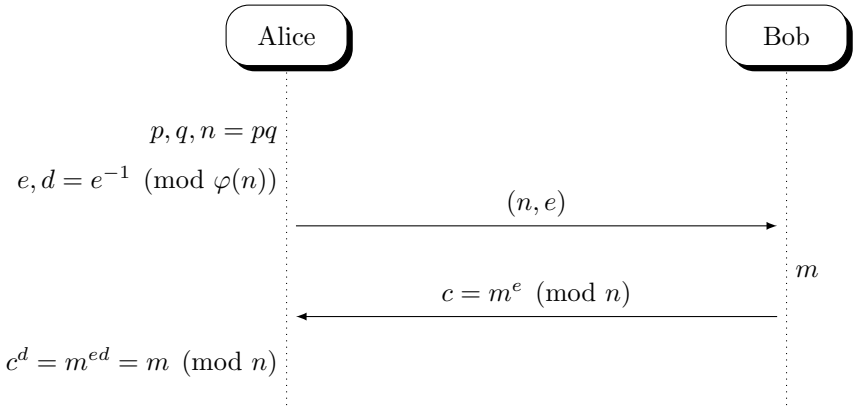


If Mallory is able to intercept the messages, she can initiate two different key exchanges, and decrypt and modify messages.

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.

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

4.1 Description

4.1.1 Groups

A *group* is a set and a binary operation $\langle G, * \rangle$ that satisfies the group axioms:

Closure For all $a, b \in G$, $a * b \in G$.

Associativity For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

Identity There exists $e \in G$ such that for all $a \in G$, $a * e = e * a = a$.

Inverse For all $a \in G$ there exists $b \in G$ such that $a * b = b * a = e$.

4.1.2 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.

4.1.3 Fields

A *field* is a set F that satisfies the field axioms:

Closure under $+$ and $\cdot$ For all $a, b \in F$, $a + b \in F$ and $a \cdot b \in F$.

Associativity of $+$ and $\cdot$ For all $a, b, c \in F$, $(a + b) + c = a + (b + c)$ and $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Commutativity of $+$ and $\cdot$ For all $a, b \in F$, $a + b = b + a$ and $a \cdot b = b \cdot a$.

Additive and Multiplicative Identities There exists a $0 \in F$ such that for all $a \in F$, $a + 0 = a$. There exists a $1 \in F$ such that for all $a \in F$, $a \cdot 1 = a$.

Additive and Multiplicative Inverses For all $a \in F$, there exists $b \in F$ such that $a + b = 0$. For all $a \in F$ $(a \neq 0)$, there exists $b \in F$ such that $a \cdot b = 1$.

Distributivity of Muliplication over Addition For all $a, b, c \in F$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

A *finite field* is a field with a finite number of elements, and is denoted $\mathbb{F}_n$ (with n elements).

$$\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$$
$$\mathbb{F}_{2^n} \cong (\mathbb{Z}/2\mathbb{Z})[x]/p(x) \text{ for irreducible } p \text{ of degree } n$$

4.1.4 Elliptic Curves over Finite Fields

Since precision is an issue with real numbers, we instead look at elliptic curves over finite fields like $\mathbb{F}_p$ and $\mathbb{F}_{2^n}$ (which can be represented in binary).

4.1.5 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.

5 Problems/Stuff to Ponder

1. Can you extend Diffie-Hellman to 3 people? 4 people? n people? Can you do it efficiently (in $O(\log n)$ exponentiations)?
2. How can you find the third point on a line passing through an elliptic curve, given 2 points on that line? What about a tangent?