Cryptography - Applications in Computer Science through Number Theory

Yongkoo Kang

1 Overview

Cryptography is a pretty broad topic, but I'm sure you're all familiar with the basic goals of cryptography: privacy, data integrity, and authentification. I'm going to cover two fairly well-known methods.

2 Diffie-Hellman Key Exchange

2.1 The Situation

Suppose you want to be able to have a common key with another individual, but only have connections with him or her through a public network. Clearly, you can't simply send one across the network due to security issues.

2.2 Solution

It turns out that there is a way to be able to share a key across a public network which will be specific to the two individuals attemping to establish a connection. However, this method does not allow for direct picking of a key due to necessary precautions in the maintenance of security.

1. Across the network, share two pieces of public data: a prime number p, to be used as a modulus, and another number b, to be used as a basis for exponentiation.
2. Individual A picks any integer, i, between 1 and p-1 to be used as an exponent.
3. A then sends the result of $b^i \% p$, let's call it D, across the network to individual B.
4. B then takes the number he has received, puts it to the power of his arbitrary number j, also between 1 and p-1, and takes it mod p ($D^j \pmod{p}$).
5. The same process is repeated with B switching roles with A.
6. The end result is that both A and B now, magically, have the same number.

2.3 Magic

At first glance, it is fairly nonintuitive as to exactly how this would work and how an outside spectator would not be able to garner similar results using his own random number. However, a simple identity dispels all doubts:

$$(b^i)^j = (b^j)^i \pmod{p}$$

From this, exactly why A and B obtain the same number is explained. For an outsider to attempt to discover exactly what number A and B now share is, he would need to solve the disecrete log problem:

$$b^i = D$$

While this is a completely solvable problem, there is no clever way to solve this equation, especially for larger numbers. Due to the nature of the operation of exponentiation then taking the modulus being very easy to do one way, but incredibly difficult to inverse, it is called a trapdoor function, one of many exploited in Cryptographic encryptions and data exchange.

3 RSA Protocol

3.1 The Situation

At this point, you want other individuals to be able to securely send you information. What should you do now?

3.2 Solution

Since this situation is an embodiment of one of the most popular areas in cryptography, this will obviously have more than one solution. However, the RSA Protocol uses the trapdoor function of multiplication, resultant of the difficulty of factoring particularly large numbers, to form a secure system.

3.2.1 Some Tools

Before entering into the specifics of the RSA Protocol, there are a few less trivial results from number theory that must be shown.

1. **Euler Totient Function:** Represented by ϕ, the totient function has a far more general form, but for the purposes of the RSA, the totient of a number expressed as pq, where p and q are both prime numbers, is given by (p-1)*(q-1) and represents the number of numbers less than or equal to pq that are relatively prime with pq. This has the very helpful property that $a^{\phi(pq)} = 1 \pmod{pq}$.

2. **Euclidean Algorithm:** This is a method for obtaining the greatest common divisor of two integers. It is a recursive algorithm in which you divide the larger argument by the smaller one and keep the remainder. Essentially, if $a > b : GCD(a, b) = GCD(a\%b, b)$. When one of the arguments becomes 0, the algorithm has been completed and the nonzero argument is the GCD.

   An expansion on the Euclidean Algorithm results in an expression for the $GCD(m, n) = am + bn$ where a and b are integers. It is essentially a back substitution.

3.2.2 The Method

1. Let individual A make an integer N, which is the product of two primes p and q, public across the network.

   For purpose of example, let N be 55, evidently 5*11.

2. Keeping in mind the fact that $\phi(N) = (p - 1)(q - 1)$, A chooses another integer less than $\phi(N)$, e, that is relatively prime to it. This item is also public.

   $\phi(55) = 4 * 10 = 40$. I will now arbitrarily choose 17.

3. Using the variant on the Euclidean Algorithm, A obtains an integer, f, which when multiplied with e taken mod $\phi(N)$ is equal to 1 ($ef = 1 \pmod{\phi(N)}$). This is kept private to only A.

   The result of the algorithm is that f should be 33.

4. As the system has now been established, individual B wants to send A a message. To do so, he takes his message M, an integer in the range 1 to N-1, and sends $M^e\%N$ to A.

   The particular message M is limited in that the $GCD(M, N) = 1$. However, for large N, this is true for a majority (approahces 100% as N gets larger).

   I want to send 4, $4^{17}\%55 = 49$, so I send 49.

5. To decode this message, A takes the the number Q he receives and puts Q to the power of f then takes it mod N ($Q^f\%N$). This results in the initial number that B had wanted to send.

   $49^{33}\%55 = 4$

3.3 Magic

There it is again! To explain what occurred, we return to the totient function and one particular identity:

$$a^{\phi(pq)} = 1 \pmod{pq}$$

By construction, $N = pq$. As such, The first number that B sends is essentially $a^e \pmod{N}$. Consequently, when A applies his own operations, the end result is: $a^{ef} \pmod{N}$. However, earlier we ensured that: $ef = 1 \pmod{\phi(N)}$. As such, ef can be represented as:

$$ef = 1 + k * \phi(N)$$

where k is an integer. Consequently:

$$a^{ef} = a^{1+k*\phi(N)}$$

which due to the first identity results in the fact that:

$$a^{ef} = a \pmod{N}.$$

which ultimately shows why this works.

3.4 Security

However, what of the malevolent spectators of this process? In such a small number case as this one, the trapdoor functionality of multiplication is not easily visible as the number 55 is trivially factorable. However, by using p and q which are hundreds of digits long, factoring of the initial N becomes almost impossible. Without the factors of N, the spectator would be unable to obtain the totient which would ultimately disallow discovery of the corresponding f value which was not revealed.