

One-Time Pad Encryption

**Presented By proidiot
DC405
December 19, 2008**

What is OTP?

- **One-Time Pad (OTP) is a very simple encryption algorithm based on modular arithmetic.**
- **Each key must be completely random and used only once.**
- **OTP is “perfectly secure” (a.k.a. “Shannon secure”) because the ciphertext provides no information about the plaintext other than the maximum possible size.**

How Does OTP Work?

- 1. Truly random keys are transferred beforehand (often in bulk in the form of a “pad”).**
- 2. The sender creates the ciphertext by using modular arithmetic on the plaintext and key a character at a time in order to calculate the corresponding character in the ciphertext. (Inside computers, this is often accomplished by a bitwise XOR on the data.)**
- 3. The sender immediately destroys his copy of the key, and then sends the ciphertext by any means to the receiver.**

A Basic OTP Implementation in C++

```
#include "../config.h"
#include "otp.hpp"
#include <string>

using namespace std;

string otp(string plaintext, string key)
{
    if (plaintext.size() > key.size()) {
        throw "Plaintext must not be larger than key.";
    }

    string ciphertext;

    for (int i = 0; i < key.size(); i++) {
        if (plaintext.size() > i) {
            // Bitwise XOR is the same as bitwise modular addition
            ciphertext.push_back(plaintext[i] ^ key[i]);
        } else {
            // We can make the plaintext the same size as the key
            // by loading extra NULLs onto the end of the plaintext
            ciphertext.push_back('\0' ^ key[i]);
        }
    }

    return ciphertext;
}
```

Why Would I Want to Use OTP?

- **OTP is one of the easiest encryption mechanisms to implement (in fact, people often do it by hand).**
- **If the keys are truly random, only used once, destroyed after use, and are transferred and kept in complete secrecy, then the ciphertext cannot be cracked (and thus “perfect secrecy” is achieved).**
- **If the above conditions are met, there is also perfect deniability.**

...Then Why Do We Use Anything Else???

- In practice, it is usually easy for others to compromise the key during transfer, while it is being stored, after it has been improperly destroyed, or all of the above.**
- True randomness in the key is almost impossible to achieve in practice.**
- Keys can only be used once.**
- Since there is no provision for message integrity, a man-in-the-middle could occur with neither party capable of knowing it.**

“Shannon Secure”

- In 1949, Claude Shannon of Bell Labs published a proof that if the keys are used only once, are completely random, and kept secure, then OTP is perfectly secure.**
- This caused the term “Shannon Secure” to be coined to refer to systems that can achieve perfect security in theory.**
- It has also been proven that anything that is Shannon Secure must have single-use keys that are used only once.**

Quantum Computing and OTP

- **True randomness is difficult to achieve as even the very few non-quantum sources of true entropy are subject to strong bias resulting from measurement.**
- **Quantum mechanics, however, gives us entropy sources that are not subject to quite as much measurement bias.**
- **Additionally, quantum entanglement would allow transfer of keys with perfect message integrity.**

What Can We Learn from OTP?

- **True randomness in encryption keys is vital.**
- **While one-time use is ideal, the closer to one-time use (such as time-sensitive keys) the better.**
- **While extremely complicated encryption algorithms aren't necessary for perfect security, algorithms that assist with the storage and transfer problems of OTP keys (such as public key mechanisms) can mean a huge step forward for practical security.**

