Cryptography Notes

20230704

The Setting of Private-Key Encryption

Encryption scheme:

- Message space $\mathcal{M}$
- 3 algorithms
  Gen Probabilistically generates a key k from some distribution
  Enc Encrypts
  Dec Decrypts

The key that the later two use is subscripted, so that $\mathbf{Dec}_k(\mathbf{Enc}_k(m)) = m$.

Kerckhoffs' principle

> *The cipher method must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience.*

Arguments:

1. Easier to keep secret
2. Easier to replace
3. Way more useful public: you get public scrutiny and compatibility guarantees

Contrast: "*Security by obscurity*"

Historical Ciphers and Their Cryptanalysis

Caesar's cipher Shift the letters of the alphabet 3 places forward (`a -> D`)

E.g.: `begin the attack now -> EHJLQWKHDWWDFNQRZ`

shift cipher Shift the letters of the alphabet k places.

Some quick C to forcebrute this:

```
#include<stdio.h>
```

```
int main()
{
    char msg[80];
    scanf("%s", msg);
    for(int i=0; i<26; i++)
    {
        char *it = msg;
        while(*it)
        {
            *it = (*it - 'A' + 1) % 26 + 'A';
            it++;
        };
        printf("%s\n", msg);
    }
}
```

Sufficient key-space principle

> *Any secure encryption scheme must have a key space that is sufficiently large to make an exhaustive-search attack infeasible.*