Cryptography

Alice wishes to communicate with Bob without Eve eavesdropping.

Private Key

In a private key system, there are two secret keys

- $e$ – the encryption key
- $d$ – the decryption key

and two functions $D$ and $E$ such that:

- for any $x$,

  $$D(E(x, e), d) = x$$

For instance, taking $d = e$ and both $D$ and $E$ as exclusive or, we have the one time pad:

$$x \oplus e \oplus e = x$$

Public Key

In public key cryptography, the encryption key $e$ is public, and the decryption key $d$ is private.

We still have,

- for any $x$,

  $$D(E(x, e), d) = x$$

If $E$ is polynomial time computable (and it must be if communication is not to be painfully slow), then the function that takes $y = E(x, e)$ to $x$ (without knowing $d$), must be in $\text{FNP}$.

Thus, public key cryptography is not provably secure in the way that the one time pad is. It relies on the existence of functions in $\text{FNP} - \text{FP}$.

One Time Pad

The one time pad is provably secure, in that the only way Eve can decode a message is by knowing the key.

If the original message $x$ and the encrypted message $y$ are known, then so is the key:

$$e = x \oplus y$$
**One Way Functions**

A function $f$ is called a *one way function* if it satisfies the following conditions:

1. $f$ is one-to-one.
2. For each $x$, $|x|^{1/k} \leq |f(x)| \leq |x|^k$ for some $k$.
3. $f \in \text{FP}$.
4. $f^{-1} \not\in \text{FP}$.

We cannot hope to prove the existence of one-way functions without at the same time proving $P \neq NP$.

It is strongly believed that the RSA function:

$$f(x, e, p, q) = (x^e \mod pq; pq; e)$$

is a one-way function.

**UP**

Though one cannot hope to prove that the RSA function is one-way without separating $P$ and $NP$, we might hope to make it as secure as a proof of $NP$-completeness.

**Definition**

A nondeterministic machine is *unambiguous* if, for any input $x$, there is at most one accepting computation of the machine.

**UP** is the class of languages accepted by unambiguous machines in polynomial time.

Equivalently, $UP$ is the class of languages of the form

$$\{x \mid \exists y R(x, y)\}$$

Where $R$ is polynomial time computable, polynomially balanced, *and* for each $x$, there is at most one $y$ such that $R(x, y)$.

We have

$$P \subseteq UP \subseteq NP$$

It seems unlikely that there are any $NP$-complete problems in $UP$.

One-way functions exist *if, and only if, $P \neq UP$.*