Random Number Generator

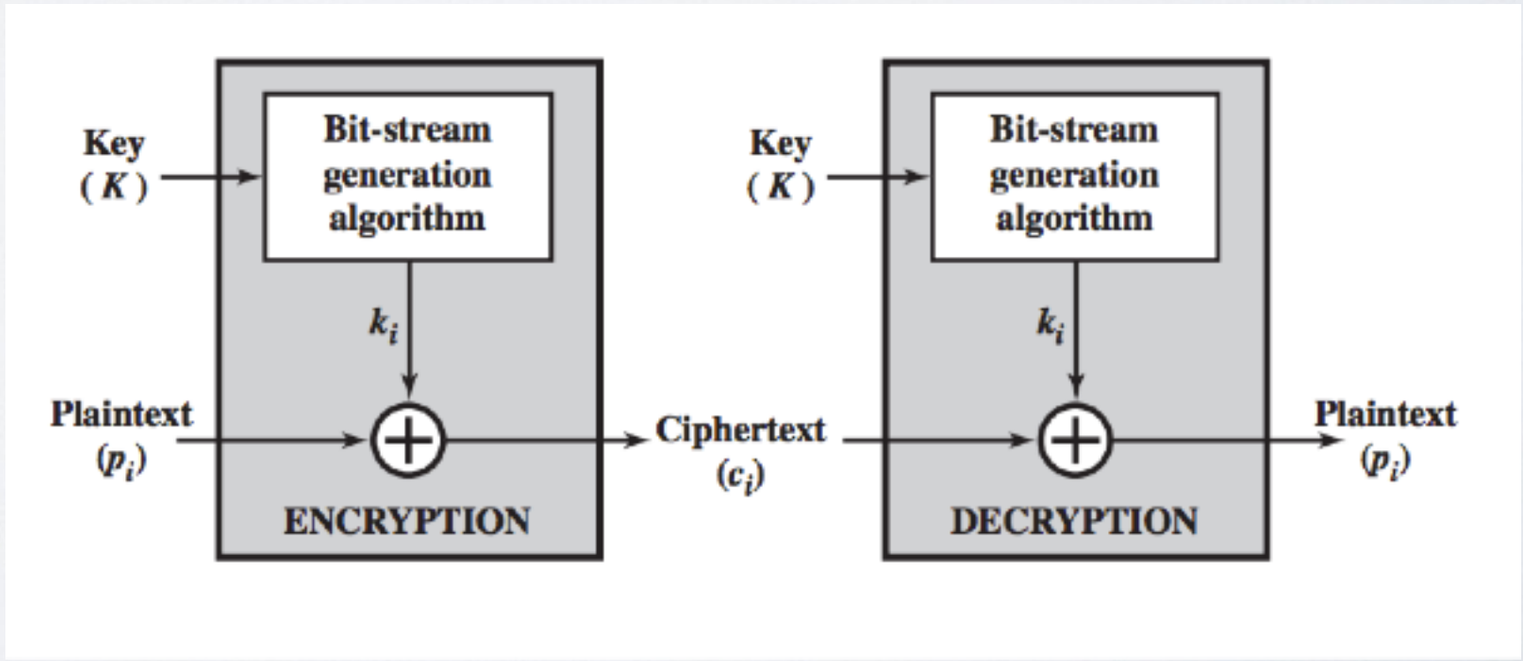
```
int getRandomNumber()
{
    return 4;  // chosen by fair dice roll.
               // guaranteed to be random.
}
```

True Random Number Generator

➡ No, because we want to be able to encrypt and decrypt

Pseudo-Random Generator

➡ Stretch a a fixed-size seed to obtain an unbounded random sequence



Stream cipher

Can we use $\mathbf{k}$ as a seed?

$$E_k(m) = m \oplus RNG(k)$$

➡ Be careful of key reused attack !

Typical usage : choose a new iv and send it using another encryption scheme E'

$$E_k(m) = (E'_k(iv)\ , m \oplus RNG(iv))$$