

Random Number Generator

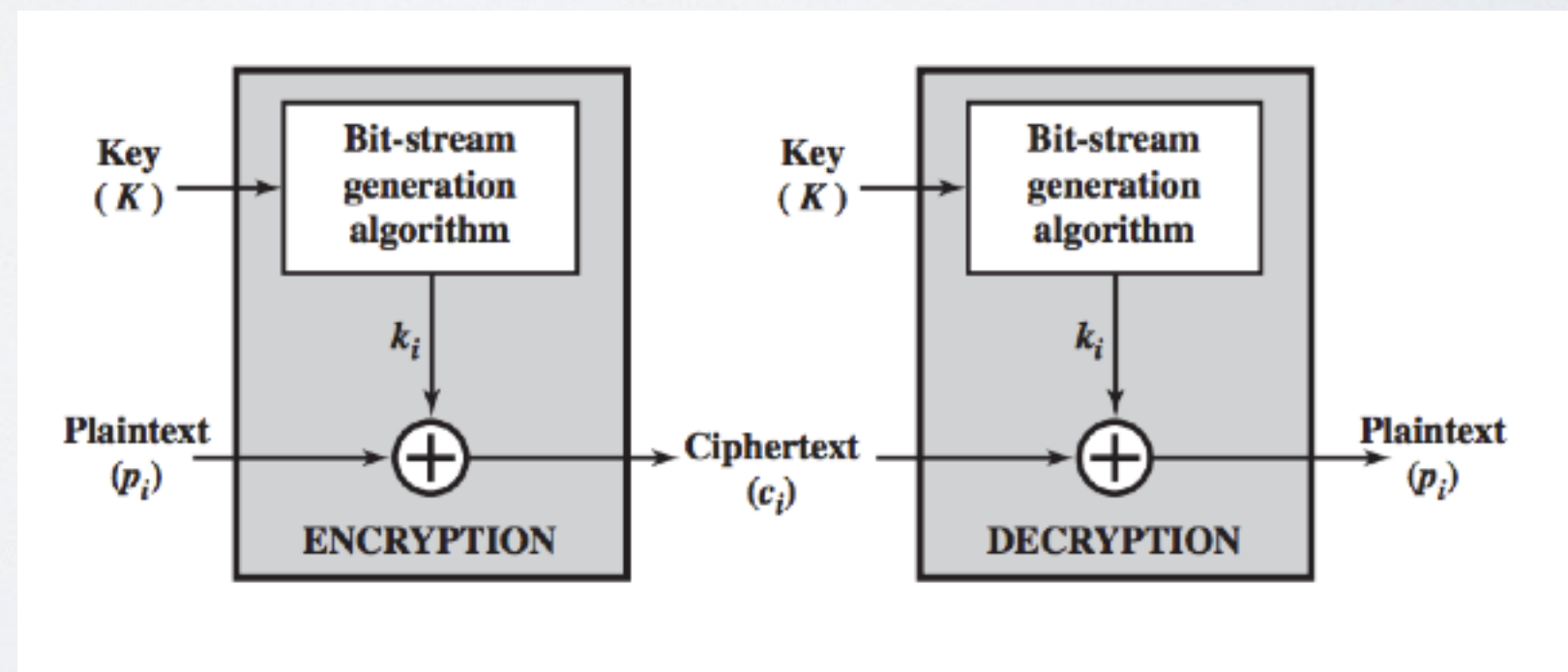
```
int getRandomNumber()  
{  
    return 4; // chosen by fair dice roll.  
             // guaranteed to be random.  
}
```

True Random Number Generator

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

Pseudo-Random Generator

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



Stream cipher

Can we use k as a seed?

$$E_k(m) = m \oplus \text{RNG}(k)$$

➡ Be careful of key reused attack !