Types of Symmetric Key Algorithms/Ciphers

Stream cipher

➡ Each bit is encrypted independently in a "stream"

RC4 - Rivest Cipher 4 (now deprecated)

Salsa20

Block cipher

➡ Blocks of data are encrypted in rounds

- Encryption standards

  DES (and 3DES) - Data Encryption Standard (now deprecated)

  AES - Advanced Encryption Standard

- Block cipher modes of operation

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