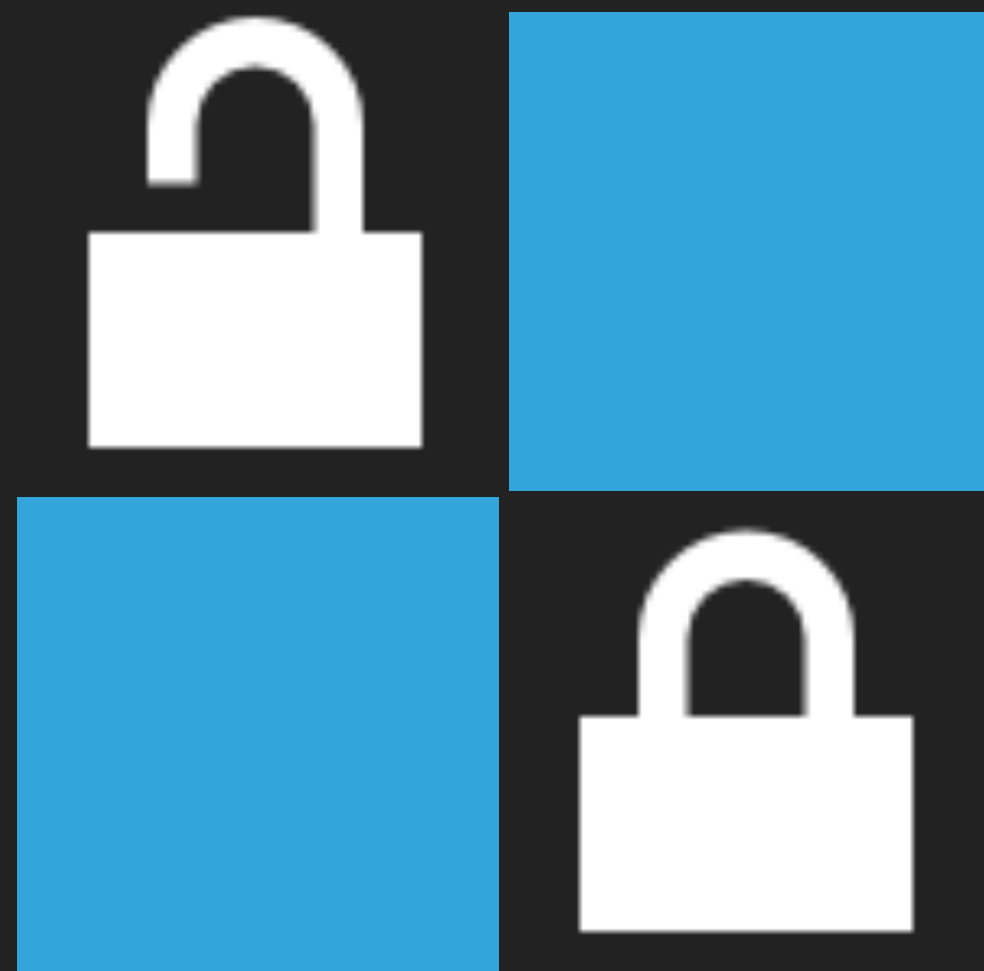


ENTROPY

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

- ▶ Bad entropy compromises keys
- ▶ Computers are very bad at making things up! (not always)
- ▶ Entropy therefore often is limited (esp. after booting!)
- ▶ Use what the API provides (SecureRandom)
- ▶ RTFM



THE FUTURE

POST QUANTUM