

1. Detecting Data Corruption

checksum = any small fixed-size function of a set of data

Simplest checksum: **XOR** (add with no carry)

data = 0x365ec4cdba148a92ecef2c3a40bef666

```
0011 0110 0101 1110 1100 0100 1100 1101
1011 1010 0001 0100 1000 1010 1001 0010
1110 1100 1110 1111 0010 1100 0011 1010
0100 0000 1011 1110 1111 0110 0110 0110
---- ---- ---- ---- ---- ---- ---- ----
0010 0000 0001 1011 1001 0100 0000 0011 = checksum = 0x201b9403
```

Can detect any single bit change.

Alternatives: add (with carry), Fletcher checksum, cyclic redundancy check (CRC), message digest (secure hash), digital signature

[checksum.py](#):

```
add = 0; xor = 0; fletcher_a, fletcher_b = 0, 0

for value in values:
    add = (add + value) % 256
    xor = xor ^ value
    fletcher_a = (fletcher_a + value) % 255
    fletcher_b = (fletcher_b + fletcher_a) % 255
```