

## Insecure

We use the standard key properties of XOR:

- It is associative
- It is commutative
- $n \oplus 0 = n$
- $n \oplus n = 0$

### Problem Solving Technique: Play

Play around with actual concrete cases on pen and paper. See if there are any patterns you can notice among them.

Here is one possible chain of logic that arrives at the solution:

- We are told that  $m = b \oplus z$ , and we know  $z$ . So we just need to find  $b$ .
- Do we have any other equations that give info about  $b$ ? Well... yes. Since  $y := b \oplus x$ , we have that  $b = y \oplus x$ , and  $x$  and  $y$  are both known!
- In summary,  $m = x \oplus y \oplus z$ .

From here, extract the bits of  $m$  in chunks of 5 (**remember to add padding zeros** to reach  $5|M|$  bits), and decode  $M$  by a lookup table.

### Implementation

For full points in C++,  $x$  and  $y$  and  $z$  will not fit in 64 bit integers anymore—they will fit in 128 bit integers like `__int128` though.

The data type `__int128` is not supported by `cin`, but it is not too hard to just read it as a string, and then convert that string into an `__int128` yourself by reading it digit-by-digit.