Unit 182
Exclusive or

The exclusive or (XOR) operation is special for cryptographers, so it deserves extra attention. Recall from Table 181.4 that its truth table is

A	B	$A \oplus B$
0	0	0
0	1	1
1	0	1
1	1	0

We also mentioned in Unit 181 that XOR is equivalent to addition modulo 2. It should therefore not surprise you that it has these properties (for all boolean variables A, B, C):

- $(A \oplus B) \oplus C = A \oplus (B \oplus C)$ (associativity) (182.1)
- $A \oplus B = B \oplus A$ (commutivity) (182.2)
- $A \oplus 0 = A$ (identity element) (182.3)
- $0 \oplus 0 = 1 \oplus 1 = 0$ (inverses)

While you would expect the above properties simple because ({TRUE, FALSE}, XOR) is an abelian group (the same as $(\mathbb{Z}_2, +_2)$), it also has some other very nice properties:

- $A \oplus 1 = \neg A$ (182.4)
- $A \oplus A = 0$ (nilpotence) (182.5)
- $A \oplus \neg A = 1$
- $A \oplus B = C \quad \Rightarrow \quad A = B \oplus C$
- $A \oplus (\neg B) = (\neg A) \oplus B = \neg (A \oplus B)$

That fourth one is important, because when we use XOR as an encryption mechanism, we can apply the same key to decipher as we use to encipher. What we mean is clearer if we replace A and B with P (plaintext) and K (key), while C denotes the ciphertext:

$$P \oplus K = C \quad \Rightarrow \quad P = C \oplus K \tag{182.6}$$

$$(P \oplus K) \oplus K = P$$

Reading and references

Any good textbook on symbolic logic.

Wikipedia: https://en.wikipedia.org/wiki/Exclusive_or

Exercises

1. Use a truth tables or manipulate equations to show that for any boolean variables *A* and *B*,
   a. $A \oplus B = (A \vee B) \wedge \neg (A \wedge B)$
   b. $A \oplus B = (A \vee B) \wedge ((\neg A) \vee (\neg B))$
   c. $(A \oplus B) \oplus B = A$
2. Use truth tables or manipulate equations to prove each of the properties of XOR listed in this unit.