Playing with $GF(2)$

Galois Field 2
has just two elements: 0 and 1

Addition is like exclusive-or:

$+$	0	1
0	0	1
1	1	0

Multiplication is like ordinary multiplication

$\times$	0	1
0	0	0
1	0	1

Evariste Galois, 1811-1832

Usual algebraic laws still hold, e.g. multiplication distributes over addition
$a \cdot (b + c) = a \cdot b + a \cdot c$

$GF(2)$ in Python

We provide a module `GF2` that defines a value `one`.
This value acts like 1 in $GF(2)$:

```
>>> from GF2 import one
>>> one + one
0
>>> one * one
one
>>> one * 0
0
>>> one/one
one
```

We will use `one` in coding with $GF(2)$.

Playing with $GF(2)$: Encryption

Alice wants to arrange with Bob to communicate one bit p (the *plaintext*).
To ensure privacy, they use a cryptosystem:

- Alice and Bob agree beforehand on a secret key k.
- Alice encrypts the plaintext p using the key k, obtaining the cyphertext c according to the table

p	k	c
0	0	0
0	1	1
1	0	1
1	1	0

Q: Can Bob uniquely decrypt the cyphertext?
A: Yes: for any value of k and any value of c, there is just one consistent value for p.

An eavesdropper, Eve, observes the value of c (but does not know the key k).
Question: Does Eve learn anything about the value of p?
Simple answer: No:

- if $c = 0$, Eve still doesn't know whether $p = 0$ or $p = 1$ since both are consistent with $c = 0$.
- if $c = 1$, Eve still doesn't know whether $p = 0$ or $p = 1$ since both are consistent with $c = 1$.

More sophisticated answer: It depends on how the secret key k is chosen.
Suppose k is chosen by flipping a coin:

Probability is $\frac{1}{2}$ that $k = 0$

Playing with $GF(2)$: Encryption

p	k	c
0	0	0
0	1	1
1	0	1
1	1	0

- Alice and Bob agree beforehand on a secret key k.
- Alice encrypts the plaintext p using the key k, obtaining the cyphertext c according to the table

Question: Does Eve learn anything about the value of p?

More sophisticated answer: It depends on how the secret key k is chosen.

Suppose k is chosen by flipping a coin:

$$\text{Probability is } \tfrac{1}{2} \text{ that } k = 0$$
$$\text{Probability is } \tfrac{1}{2} \text{ that } k = 1$$

There are two possibilities:

- Suppose $p = 0$. Then (looking at first two rows of encryption table)
$$\text{Probability is } \tfrac{1}{2} \text{ that } c = 0$$
$$\text{Probability is } \tfrac{1}{2} \text{ that } c = 1$$
- Now suppose $p = 1$. Then (looking at last two rows of encryption table)
$$\text{Probability is } \tfrac{1}{2} \text{ that } c = 1$$
$$\text{Probability is } \tfrac{1}{2} \text{ that } c = 0$$

Thus the choice of the value of p does not affect the probability distribution of c.

This shows that Eve learns nothing about p from observing c. Perfect secrecy!

Playing with $GF(2)$: One-to-one and onto function and perfect secrecy

What is it about this cryptosystem that leads to perfect secrecy? Why does Eve learn nothing from eavesdropping?

p	k	c
0	0	0
0	1	1
1	0	1
1	1	0

Define $f_0 : GF(2) \longrightarrow GF(2)$ by

$f_0(k) =$encryption of $p = 0$ with key k

According to the first two rows of the table,

$$f_0(0) = 0 \text{ and } f_0(1) = 1$$

$\boxed{\text{This function is one-to-one and onto.}}$

When key k is chosen uniformly at random

$$\text{Prob}[k = 0] = \tfrac{1}{2}, \text{Prob}[k = 1] = \tfrac{1}{2}$$

the probability distribution of the output $f_0(k) = p$ is also uniform:

$$\text{Prob}[f_0(k) = 0] = \tfrac{1}{2}, \text{Prob}[f_0(k) = 1] = \tfrac{1}{2}$$

Define $f_1 : GF(2) \longrightarrow GF(2)$ by

$f_1(k) =$encryption of $p = 1$ with key k

According to the last two rows of the table,

$$f_1(0) = 1 \text{ and } f_1(1) = 0$$

$\boxed{\text{This function is one-to-one and onto.}}$

When key k is chosen uniformly at random

$$\text{Prob}[k = 0] = \tfrac{1}{2}, \text{Prob}[k = 1] = \tfrac{1}{2}$$

the probability distribution of the output $f_1(k) = p$ is also uniform:

$$\text{Prob}[f_1(k) = 1] = \tfrac{1}{2}, \text{Prob}[f_1(k) = 0] = \tfrac{1}{2}$$

The probability distribution of the cyphertext does not depend on the plaintext!

Perfect secrecy

Idea is the basis for cryptosystem: the **one-time pad**.

If each bit is encrypted with its own one-bit key, the cryptosystem is unbreakable

p	k	c
0	0	0
0	1	1
1	0	1
1	1	0

In the 1940's the Soviets started re-using bits of key that had already been used.

Unfortunately for them, this was discovered by the US Army's Signal Intelligence Service in the top-secret VENONA project.

This led to a tiny but historically significant portion of the Soviet traffic being cracked, including intelligence on

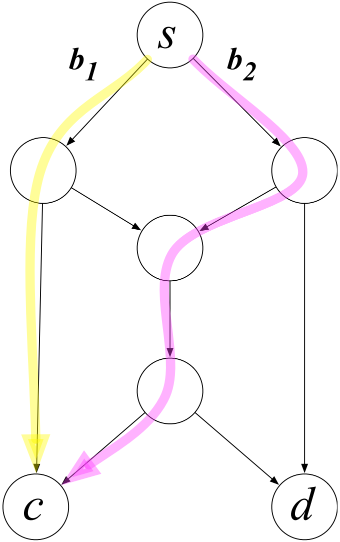
- spies such as Julius Rosenberg and Donald Maclean, and
- Soviet espionage on US technology including nuclear weapons.

The public only learned of VENONA when it was declassified in 1995.

Playing with $GF(2)$: Network coding

Streaming video through a network

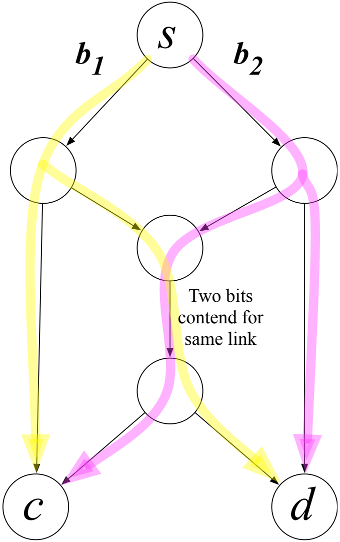
- one customer—no problem
- two customers—contention! ☹
- do computation at intermediate nodes — avoids contention
- Network coding doubles throughput in this example!



Playing with $GF(2)$: Network coding

Streaming video through a network

- one customer—no problem
- two customers—contention! ☹
- do computation at intermediate nodes — avoids contention
- Network coding doubles throughput in this example!



Playing with $GF(2)$: Network coding

Streaming video through a network

- one customer—no problem
- two customers—contention! ☹
- do computation at intermediate nodes — avoids contention
- Network coding doubles throughput in this example!