

# Kerckhoff's Principle (1883)

A cryptosystem should be secure when the attacker knows all the details of the encryption and decryption algorithms but does not know the secret key.

i.e. No security through obscurity of the method

1. Verify this is multiplication table for  $\mathbb{Z}_7$

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

2. Calculate in  $\mathbb{Z}_7$

(a)  $3 - 5$ ,  $-2 - 3$

(b)  $4 \cdot 3^{-1}$ ,  $2 \cdot 4^{-1}$

(c)  $3^2$ ,  $3^3$ ,  $3^4$ ,  $3^5$ ,  $3^6$ ,  
 $3^{12}$ ,  $3^{21}$

3. Solve for  $x$

(a)  $3^x \equiv 5 \pmod{7}$

(b)  $5^x \equiv 2 \pmod{7}$

(c)  $2^x \equiv 3 \pmod{7}$