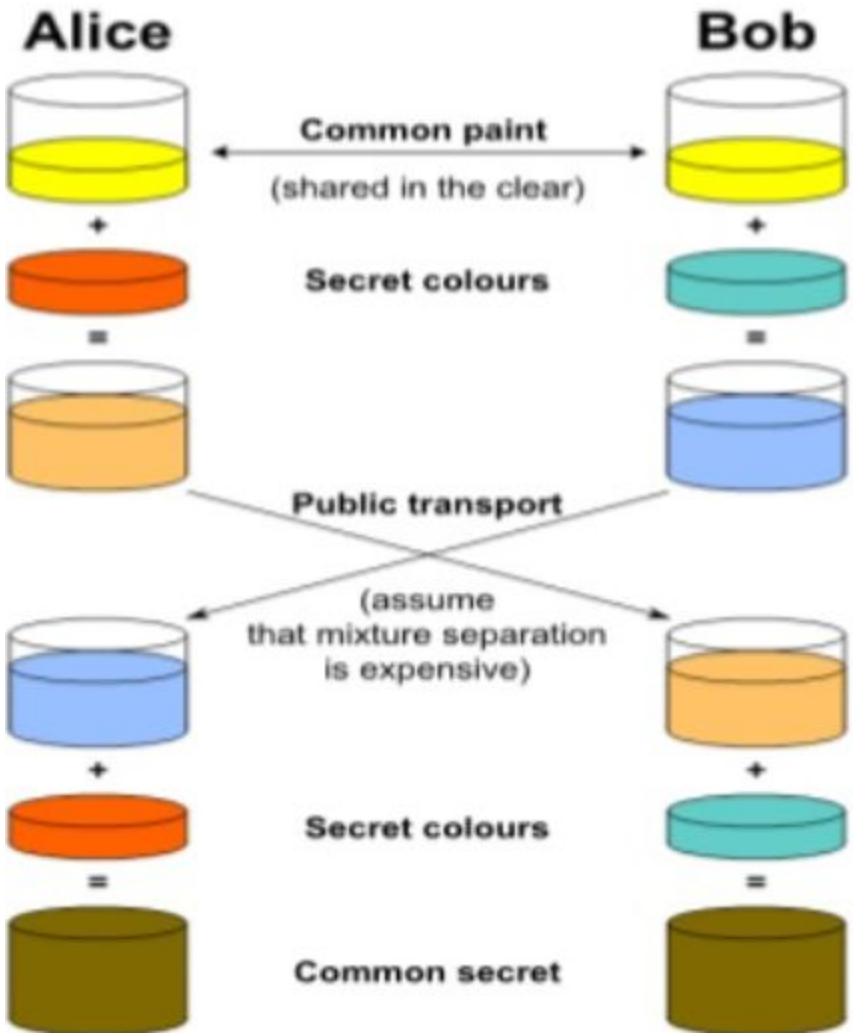
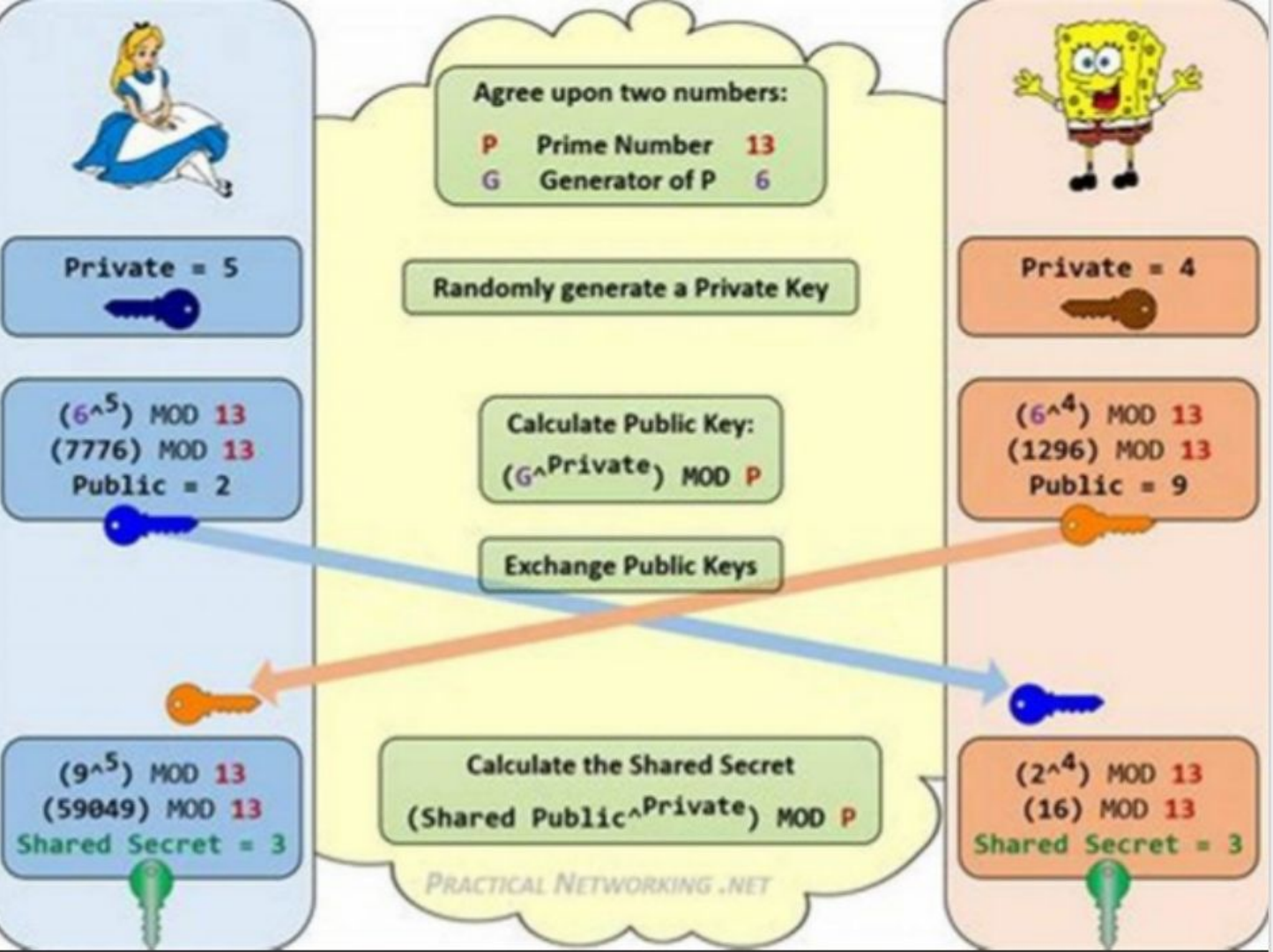
Diffie-Hellman Algorithm


Alice
Bob
Common paint
(shared in the clear)
Secret colours
Public transport
(assume
that mixture separation
is expensive)
Secret colours
Common secret



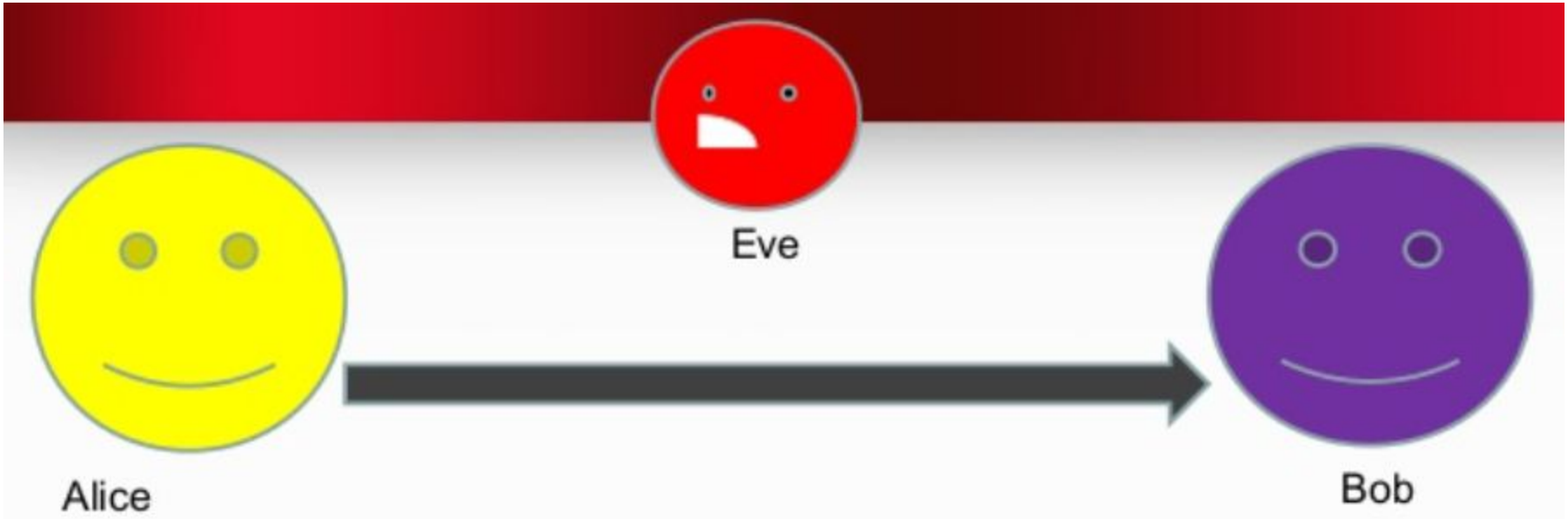
$$[6^{5}]^{4} = [6^{4}]^{5}$$

A^B mod C =

((A mod C)^B) mod C

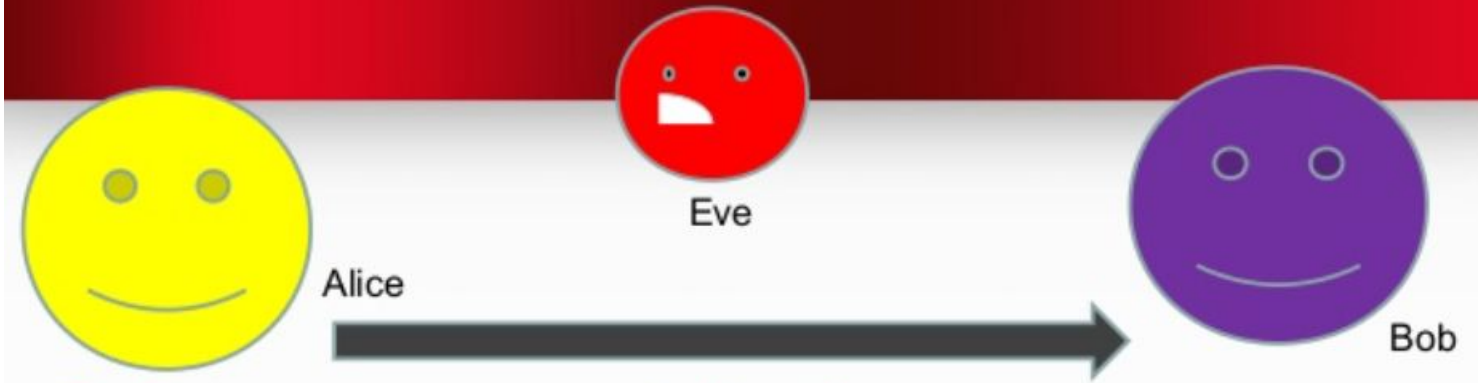
History

- The Diffie-Hellman algorithm was developed by Whitfield Diffie and Martin Hellman in 1976.
- This algorithm was devices not to encrypt the data but to generate same private cryptographic key at both ends so that there is no need to transfer this key from one communication end to another.



- The first step in public-key cryptography Alice and Bob want exchange an encryption key over an insecure communication link where Eve is listening in.

Step 1: Alice and Bob agree on a prime number P.
P = 5



Step 2: Alice and Bob agree on a primitive root of their prime number.
Let us test if the number 3 is a primitive root of 5.
g^(positive whole number less than our P)
3^1=3
3^2=9
3^3=27
3^4=81
Then we set our upper limit of our output to the value of our prime, by getting the remainder after division.
3 mod 5 = 3
9 mod 5 = 4
27 mod 5 = 2
81 mod 5 = 1. So now that we have found our primitive root we will note its value. g = 3

α is a primitive root of q if:

$$\alpha \bmod q, \alpha^2 \bmod q, \alpha^3 \bmod q, \ldots\ldots \alpha^{q-1} \bmod q$$

1, 2, 3, ... q-1

Primitive Root

Given a prime number n, the task is to find its primitive root under modulo n. The primitive root of a prime number n is an integer r between[1, n-1] such that the values of r^x(mod n) where x is in the range[1, n-1] are different.

```
Input : 7

Output : Smallest primitive root = 3

Explanation: n = 7

3^1(mod 7) = 3

3^2(mod 7) = 2

3^3(mod 7) = 6

3^4(mod 7) = 4

3^5(mod 7) = 5

3^6(mod 7) = 1
```

Primitive Root

$\gcd(4, 7) = 1$

$7 \longrightarrow \underbrace{1, 2, 3, 4, 5, 6}$

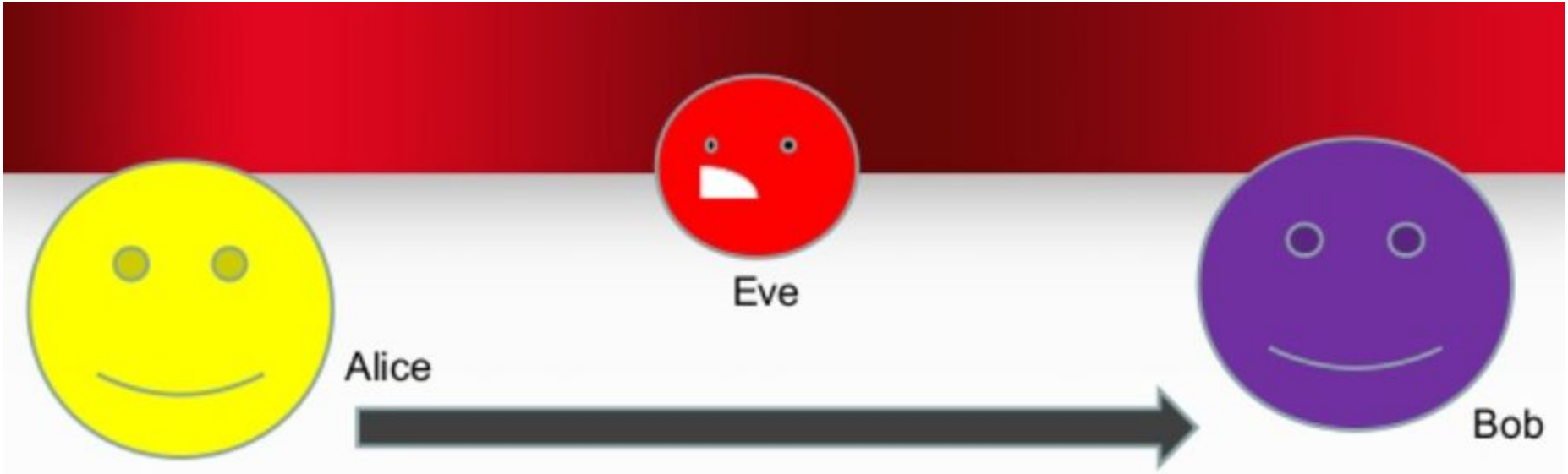
$a^{1-6} \bmod 7 \longrightarrow 1, 2, 3, 4, 5, 6.$

a ↓	a^1	a^2	a^3	a^4	a^5	a^6	(mod 7)
1	1	1	1	1	1	1	X
2	2	4	1	2	4	1	X
3	3	2	6	4	5	1	✓
4	4	2	1	4	2	1	X
5	5	4	6	2	3	1	✓
6	6	1	6	1	6	1	X

$6^1 \equiv 6 \bmod 7$

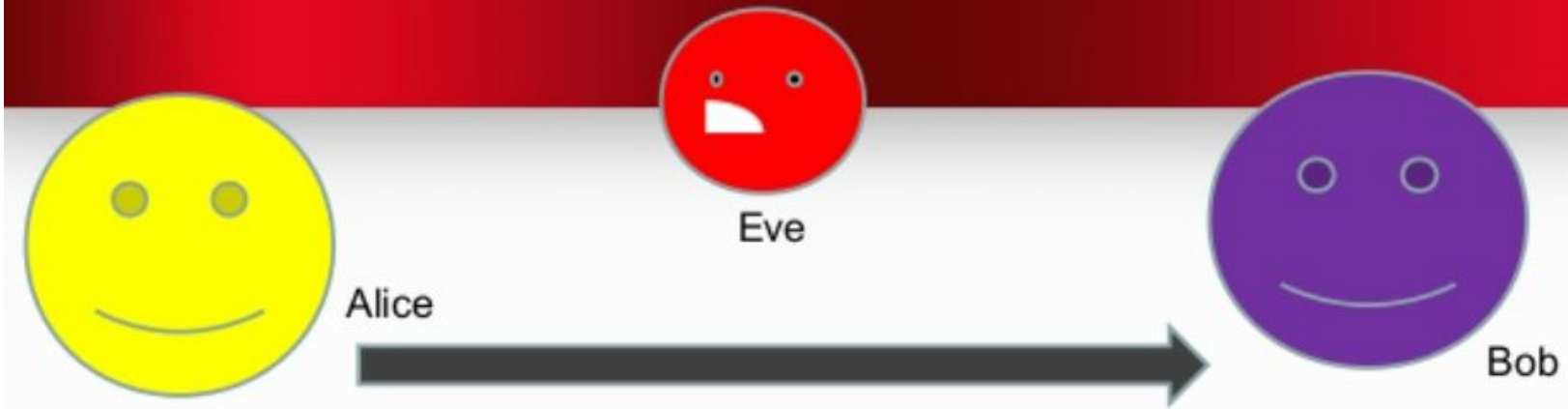
$6^2 \equiv (36 - 35) \equiv 1$

$3, 5 \longrightarrow 7$



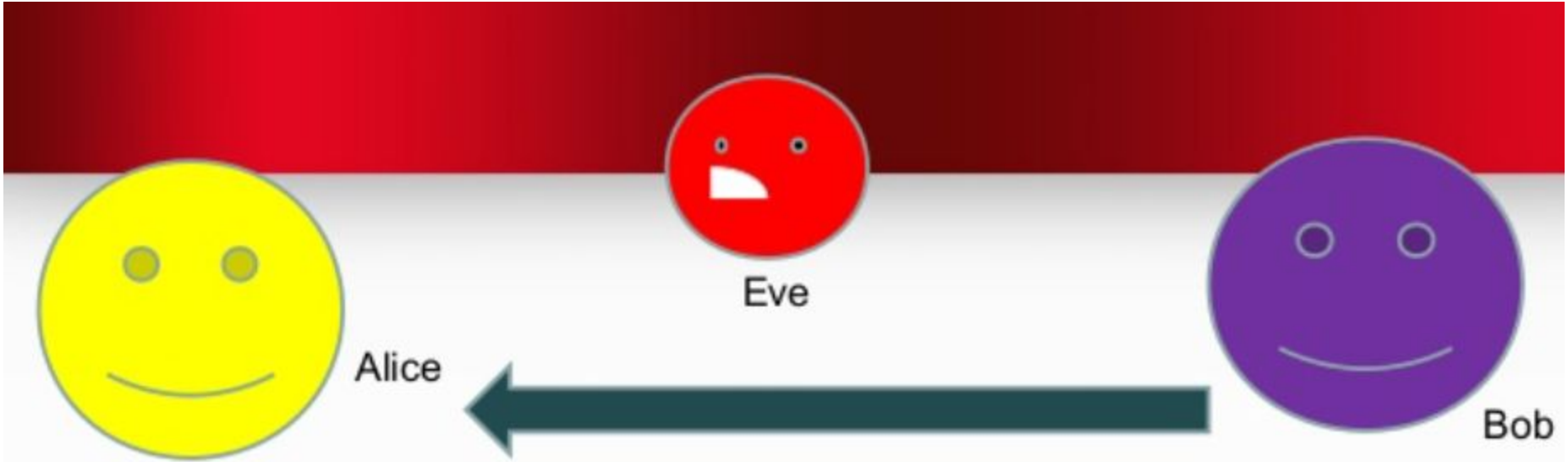
Step 3: Alice chooses a positive whole number as her secret key.
a = 6

Step 4: Alice computes her public key and sends it to Bob.
A = g^a mod P or
A = 3^6 mod 5
A = 4



Step 5: Bob chooses a positive whole number as his secret key.
b = 7

Step 6: Bob computer his public key and sends it to Alice.
B = g^b mod P
B= 3^7 mod 5
B = 2



Step 7: Alice and Bob now compute a shared secret key

[Shared Key] = [other persons public key]^[their own secret key] mod P

Bob: S = 4^7 mod 5

Alice: S = 2^6 mod 5

S = 4

Modular Arithmetic

Modular exponentiation

A^B mod C = ((A mod C)^B) mod C

Modular Arithmetic

Modular operator

-29 mod 3 = 1

-14 mod 2 = 0

-4 mod 9 = 5

-17 mod 7 = 4

Modular Arithmetic

Congruence modulo

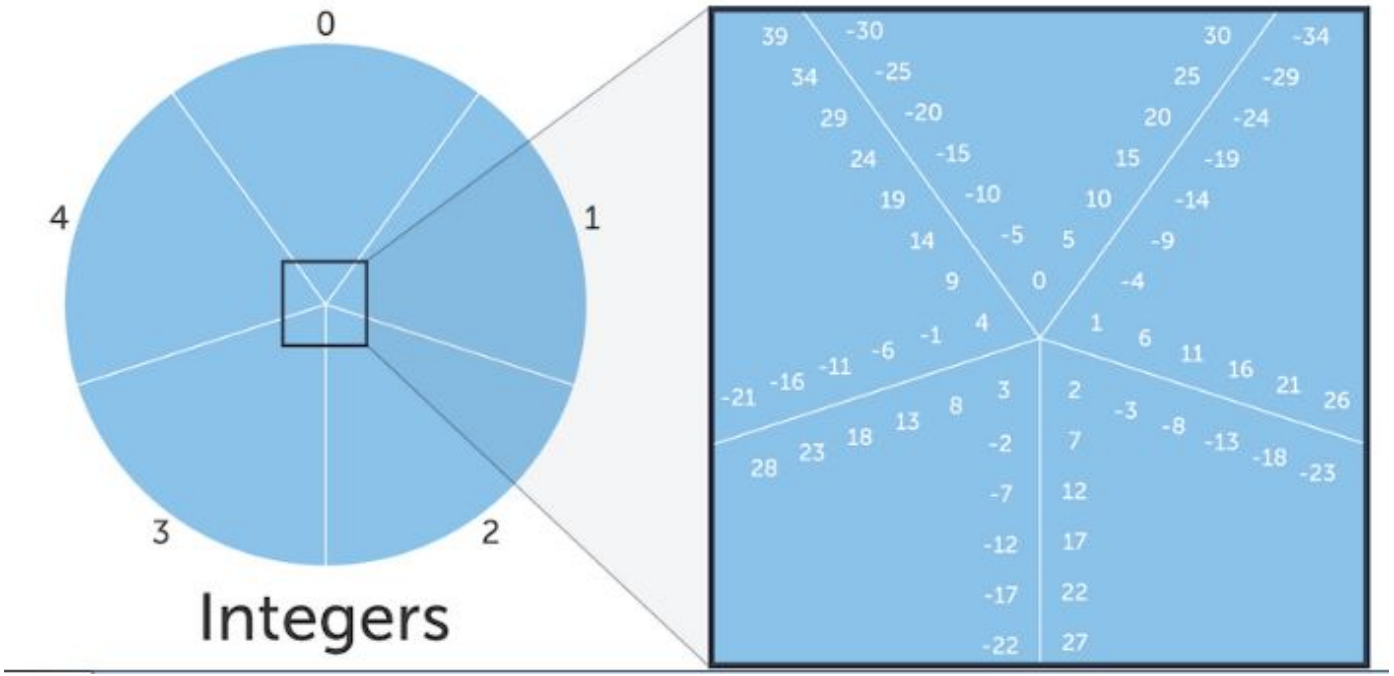
$$A \equiv B \pmod{C}$$

This says that A is **congruent** to B modulo C.

Modular Arithmetic

Congruence modulo

Let's imagine we were calculating mod 5 for all of the integers:



Modular Arithmetic

Congruence modulo

$$A \equiv B \pmod{C}$$

e.g. $26 \equiv 11 \pmod{5}$

$26 \bmod 5 = 1$ so it is in the equivalence class for 1,

$11 \bmod 5 = 1$ so it is in the equivalence class for 1, as well.

$\equiv$ is the symbol for congruence, which means the values A and B are in the same **equivalence class**.

Modular Arithmetic

Modular multiplication

$$(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$$

Modular Arithmetic

Modular addition, subtraction

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$

$$(A - B) \bmod C = (A \bmod C - B \bmod C) \bmod C$$

Modular Arithmetic

What is a modular inverse?

In modular arithmetic we do not have a division operation. However, we do have modular inverses.

- The modular inverse of A (mod C) is A^-1
- (A * A^-1) ≡ 1 (mod C) or equivalently (A * A^-1) mod C = 1
- Only the numbers coprime to C (numbers that share no prime factors with C) have a modular inverse (mod C)

Modular Arithmetic

Modular inverse

Example: A=3, C=7

Step 1. Calculate A * B mod C for B values 0 through C-1

$3 * 0 \equiv 0 \pmod 7$

$3 * 1 \equiv 3 \pmod 7$

$3 * 2 \equiv 6 \pmod 7$

$3 * 3 \equiv 9 \equiv 2 \pmod 7$

$3 * 4 \equiv 12 \equiv 5 \pmod 7$

$3 * 5 \equiv 15 \pmod 7 \equiv 1 \pmod 7$ <------ FOUND INVERSE!

$3 * 6 \equiv 18 \pmod 7 \equiv 4 \pmod 7$

5 is the modular inverse of 3 mod 7 since 5*3 mod 7 = 1

$27^{-1} \pmod{392}$

$392 = 27 \cdot (14) + 14$

$27 = 14 \cdot (1) + 13$

$14 = 13 \cdot 1 + 1$

$14 + 13(-1) = 1$

$(27 + 14(-1)) = 13$

$[392 + 27(-14)] = 14$

$392 - 29 = 363$

$(1) \cdots 14 + [27 + 14(-1)](-1) = 1$

$14 + 27(-1) + 14 = 1$

$2(14) + 27(-1) = 1$

$2[392 + 27(-14)] + 27(-1) = 1$

$2 \cdot 392 + 27(-28) + 27(-1) = 1$

$2 \cdot 392 + 27(-29) = 1 \pmod{392}$

$2 \cdot 392^{0} + 27 \cdot 363 = 1 \pmod{392}$

$27 \cdot 363 = 1 \pmod{392}$

$363 = \frac{1}{27} = 27^{-1} \pmod{392}$