Ассиметричное шифрование

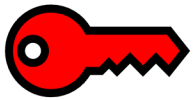
RSA

Отпредение

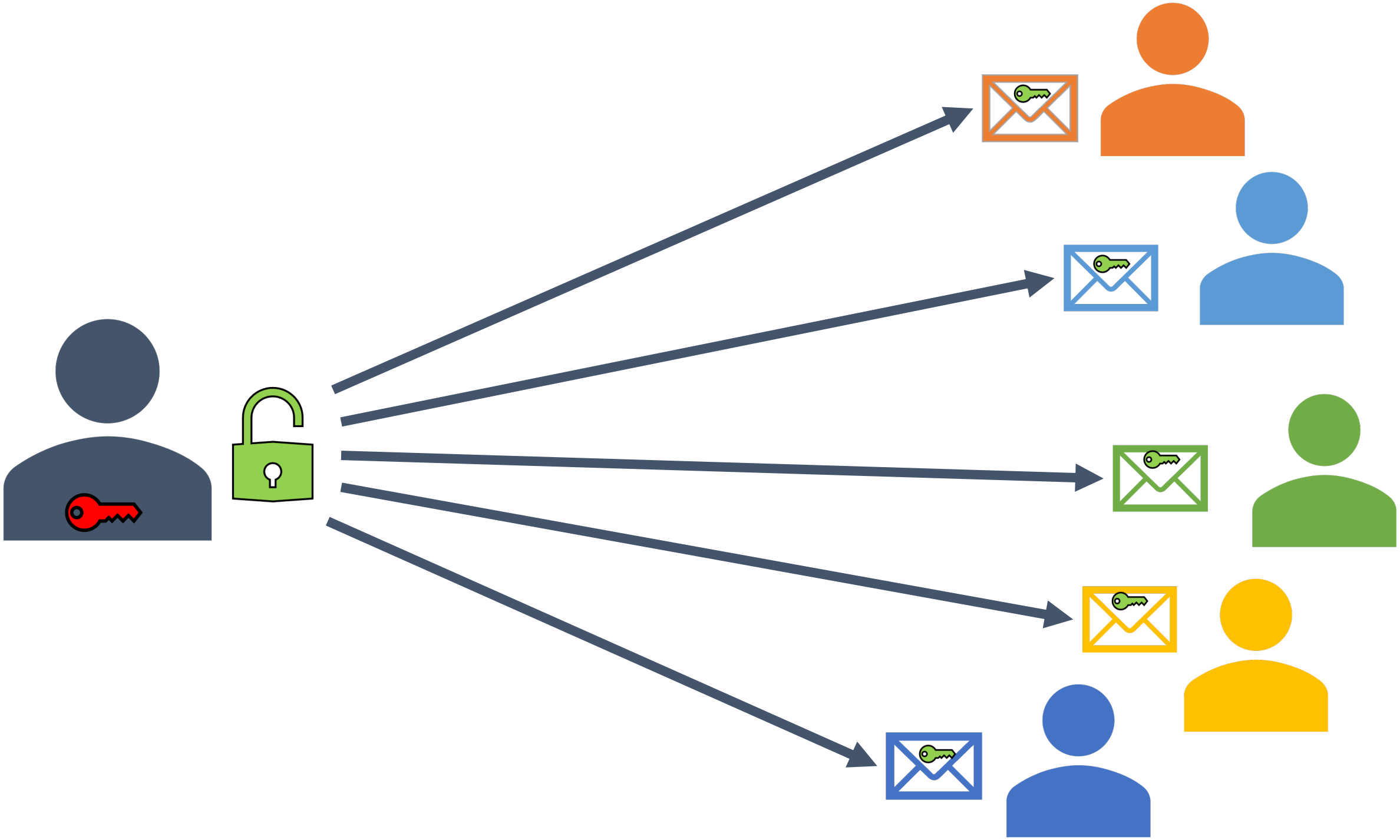
Шифрование с открытым ключом, в котором для шифрования и расшифрования применяются разные ключи. Причем один, не может быть простым способом получен из другого.

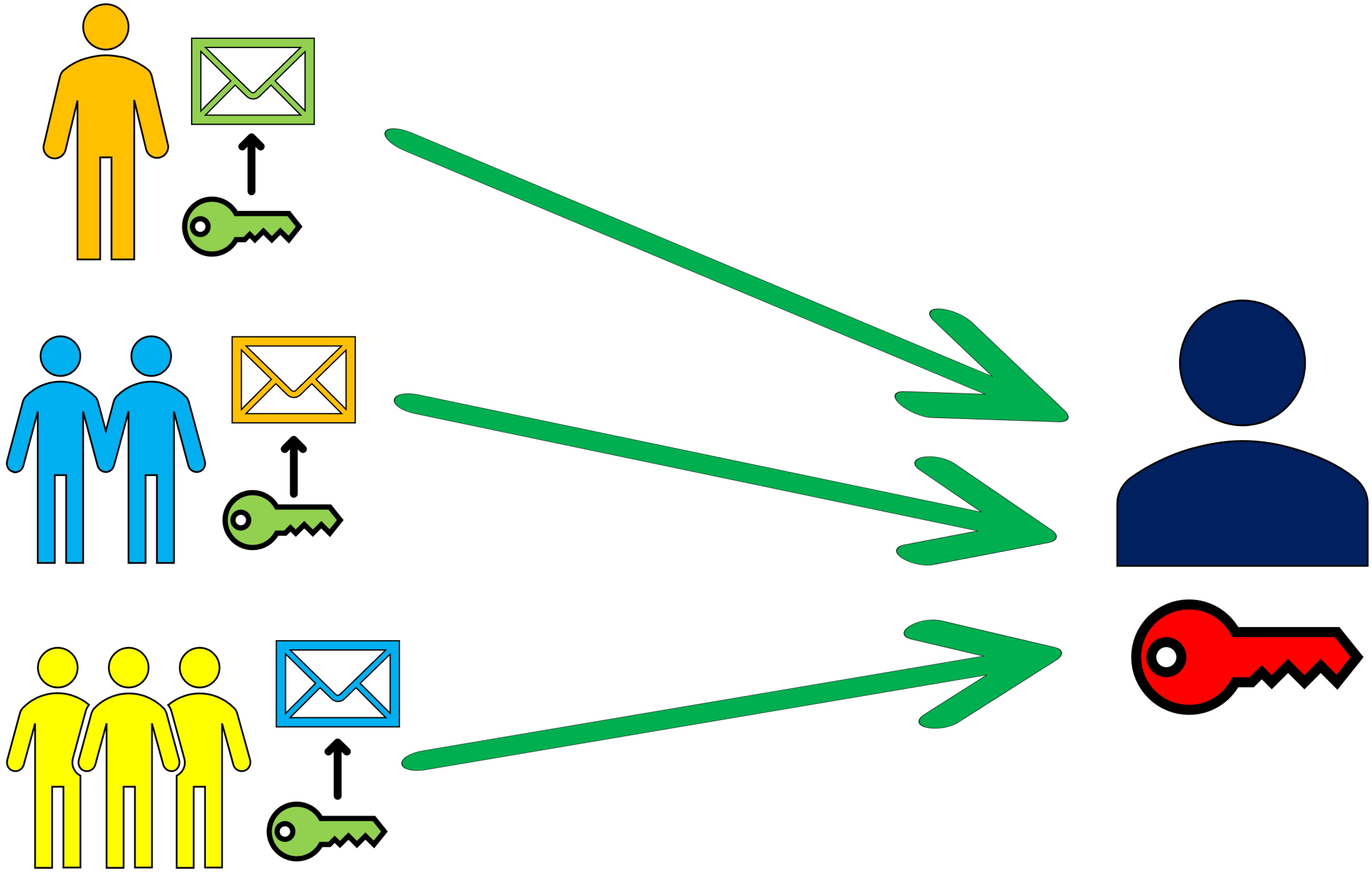
Ключи

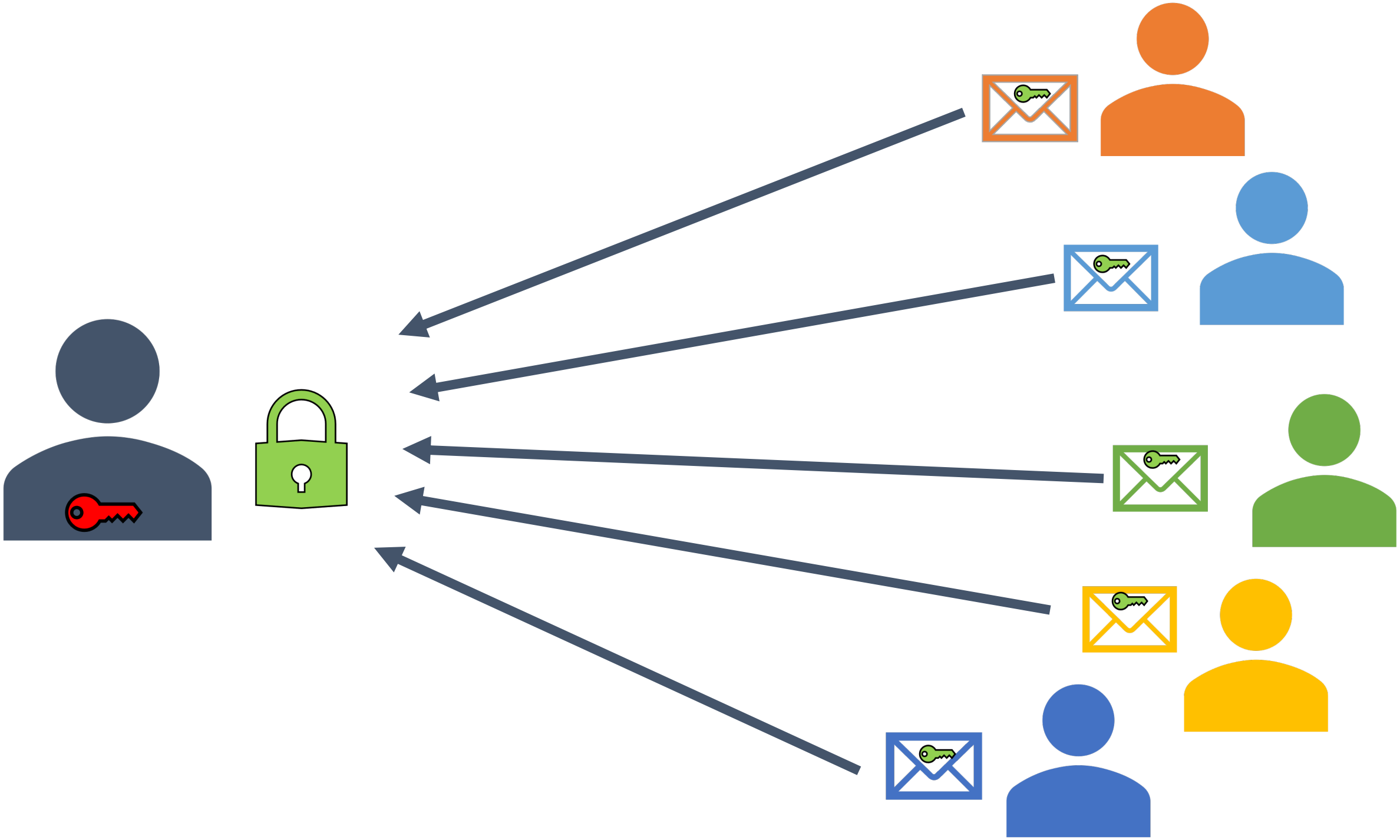
- Открытый(публичный) ключ – это ключ, который известен каждому и не является секретной частью алгоритма шифрования. С его помощью, любой желающий может зашифровать сообщение.

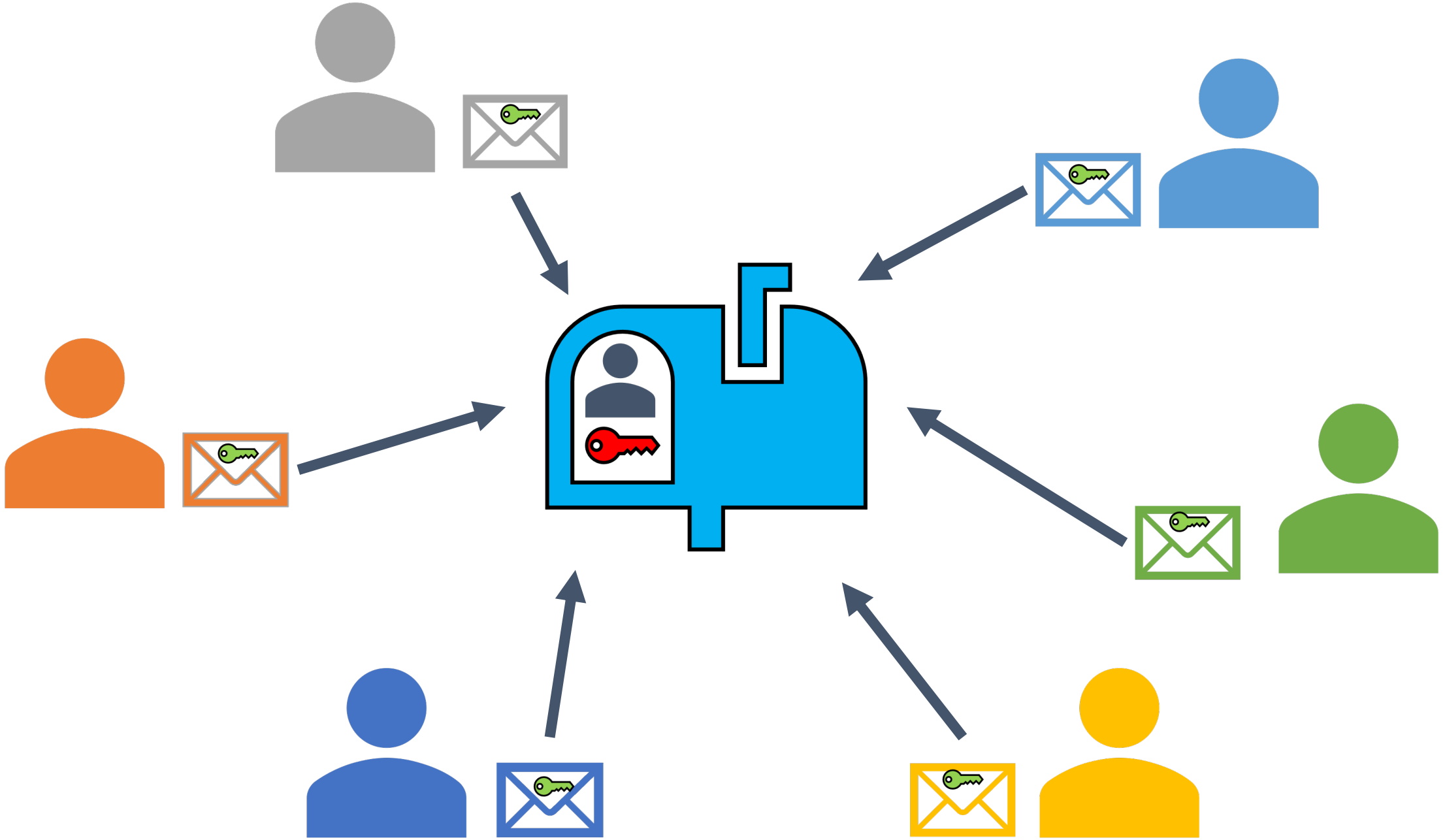


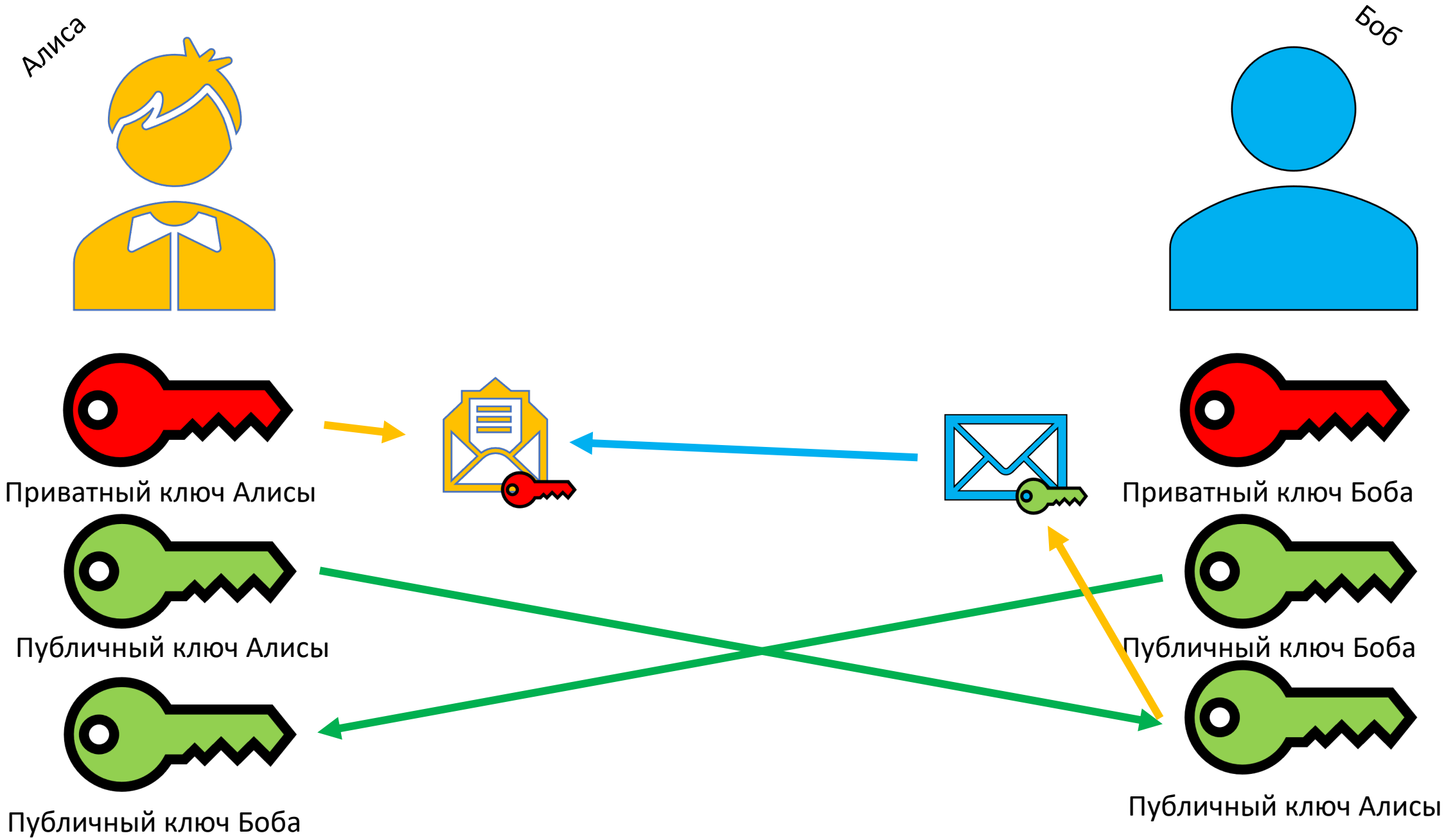
- Закрытый ключ – это часть алгоритма, которая является секретной, только обладая этим ключом можно расшифровать сообщение, полученное с помощью открытого ключа и криптографического преобразования.



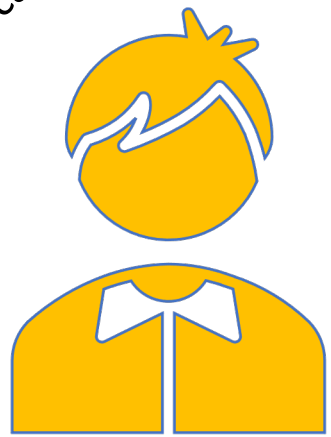




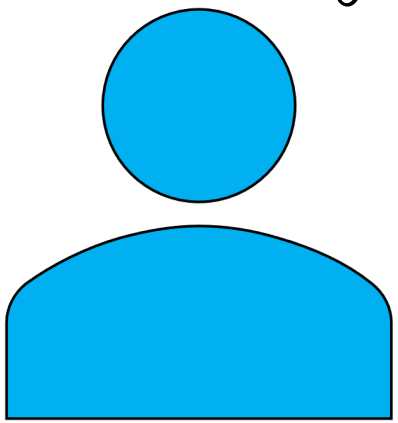



Алиса
Боб
Приватный ключ Алисы
Публичный ключ Алисы
Публичный ключ Боба
Приватный ключ Боба
Публичный ключ Боба
Публичный ключ Алисы

Алиса



Боб



N = 89

p1 = 53
P2 = 59

n = p1 * p2 = 53 * 59

n = 3127 

Φ(n) = (p1 – 1) * (p2 – 1) = 52 * 58

Φ(n) = 3016

e = (простое, не имеет делителя с Φ(n) > e)

e = 3 

$N^e \ mod \ n$ = c

$89^3 \ mod \ 3127$ = 1394

c = 1394

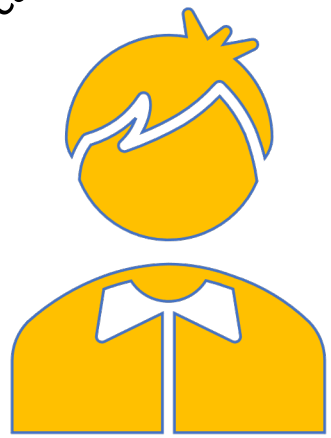
d = $\frac{2 * \Phi(n) + 1}{e} = \frac{2 * (3016) + 1}{3}$ (d * e) mod Φ(n) = 1

d = 2011 

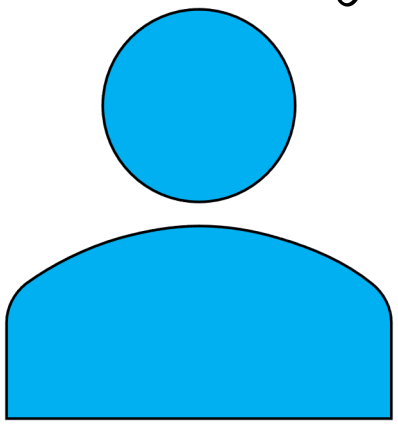
$c^d mod \ n = N$

$1394^{2011} mod \ 3127 = 89$

Алиса



Боб



p1 = 53
P2 = 59
n = p1 * p2 = 53 * 59
n = 3127

Φ(n) = (p1 – 1) * (p2 – 1) = 52 * 58
Φ(n) = 3016
e = (не четное, не имеет делителя с Φ(n))
e = 3

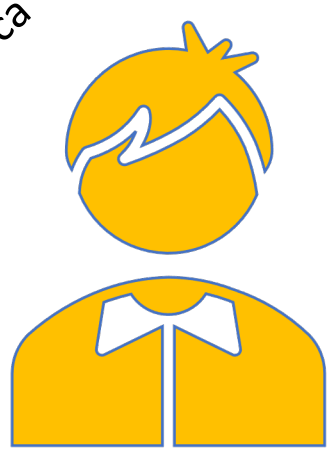
$$d = \frac{2 * \Phi(n) + 1}{e} = \frac{2 * (3016) + 1}{3}$$

d = 2011

Hello

H = 8
E = 5
L = 12
O = 15

Алиса



d = 2011

$c^d mod\ n = N$

$512^{2011} mod\ 3127 = 8\ (H)$

$125^{2011} mod\ 3127 = 5\ (E)$

$1728^{2011} mod\ 3127 = 12\ (L)$

$1728^{2011} mod\ 3127 = 12\ (L)$

$248^{2011} mod\ 3127 = 15\ (O)$

$N^e\ mod\ n$ = c

$8^3\ mod\ 3127$ = 512

$5^3\ mod\ 3127$ = 125

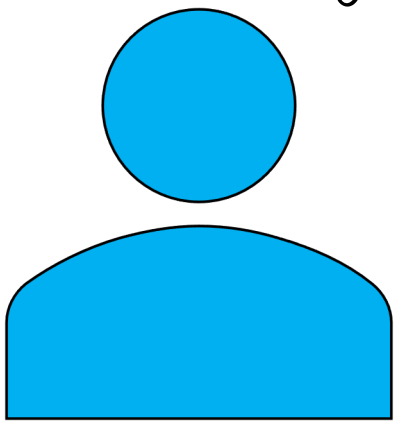
$12\ mod\ 3127$ = 1728

$12\ mod\ 3127$ = 1728

$15^3\ mod\ 3127$ = 248

c = 512, 125, 1728, 1728, 248

Боб



Hello

H = 8 L = 12

E = 5 O = 15