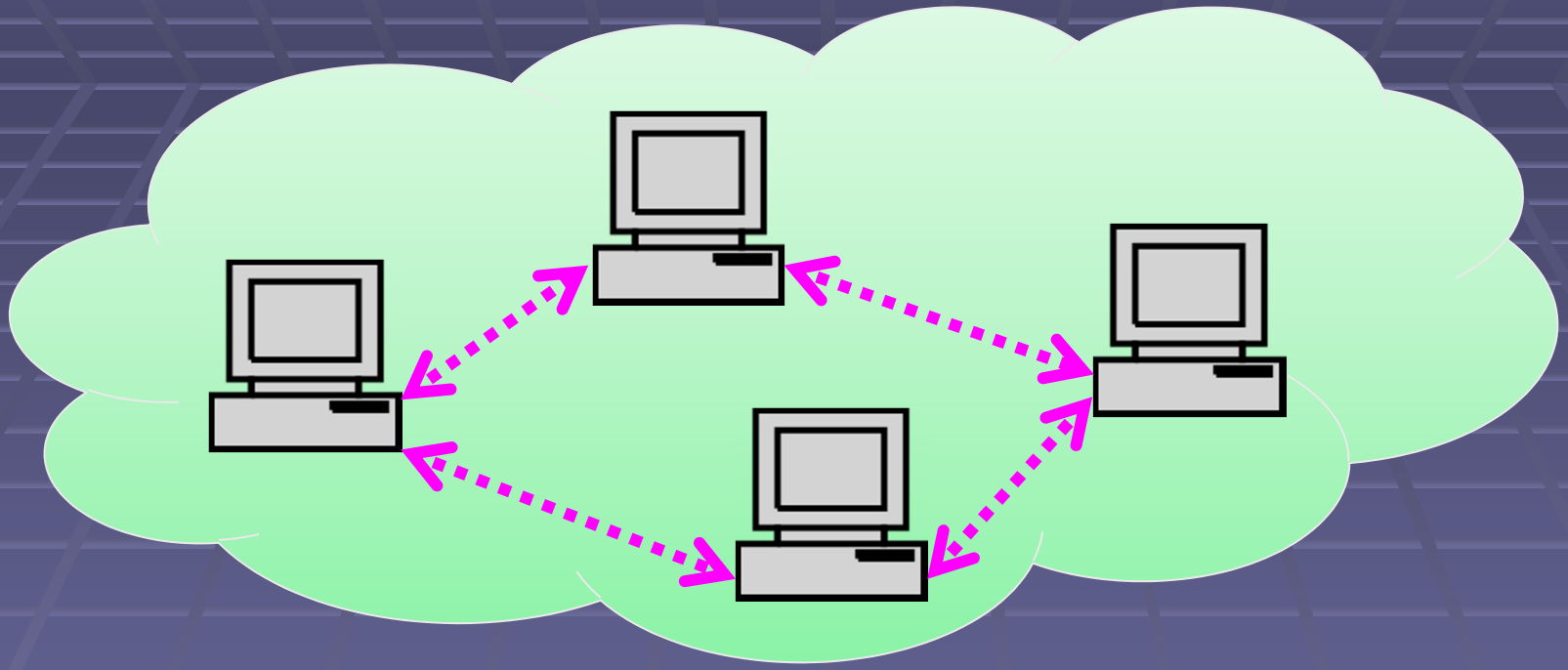
Гомоморфное шифрование: священный Грааль криптографии

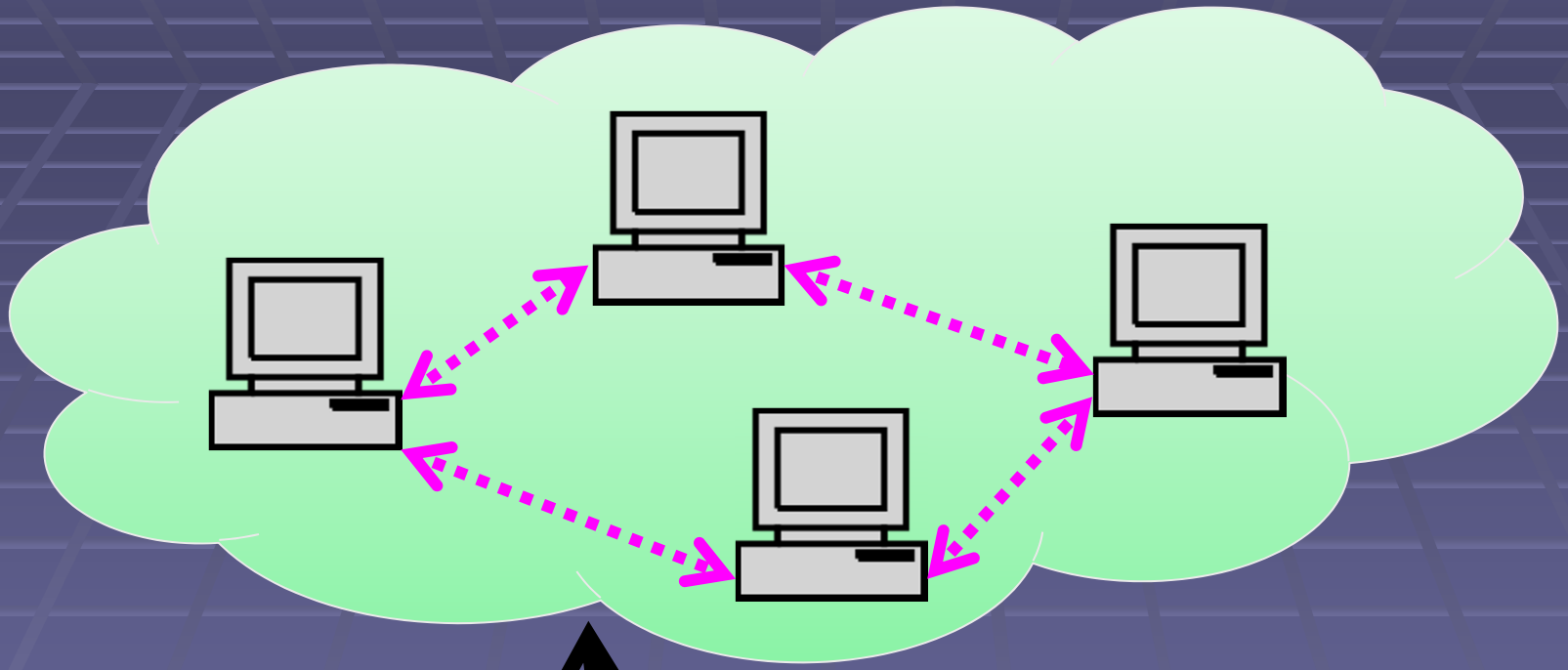
Владимир Захаров

ф-т ВМК МГУ

Облачные вычисления



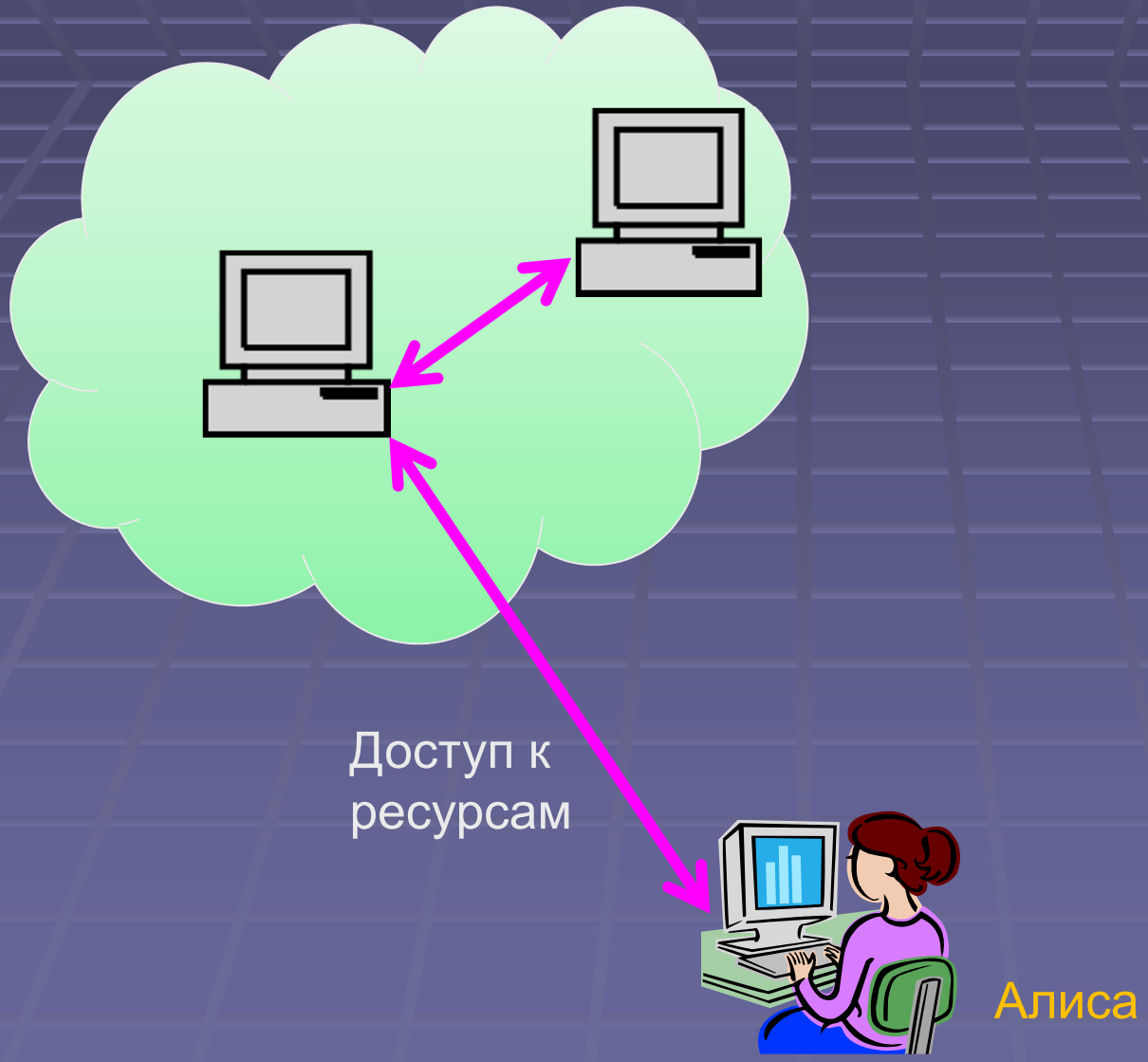
Облачные вычисления



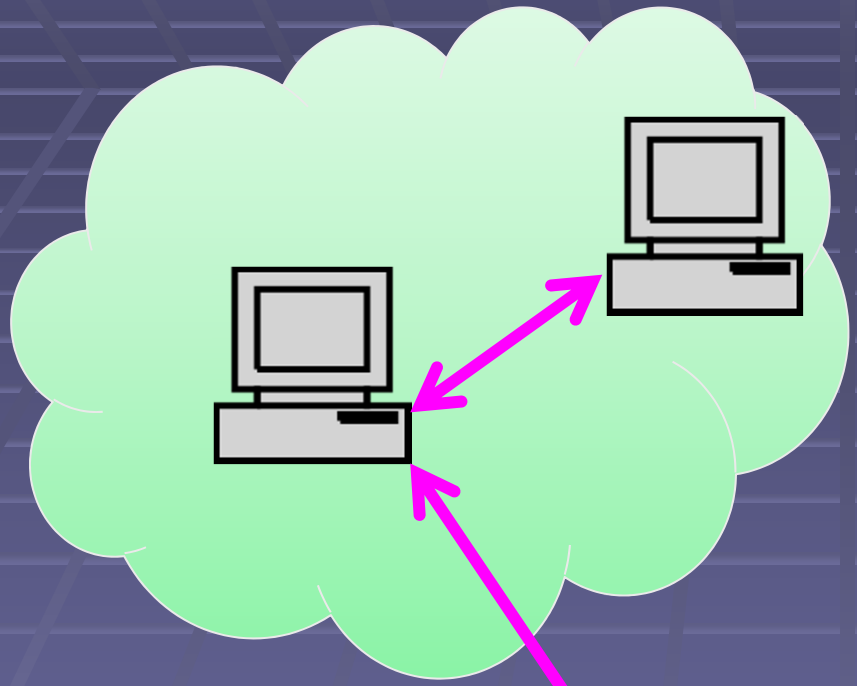
Запрос на вычислительные ресурсы

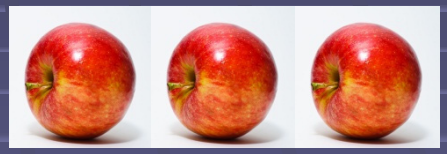
Алиса

Облачные вычисления



Облачные вычисления

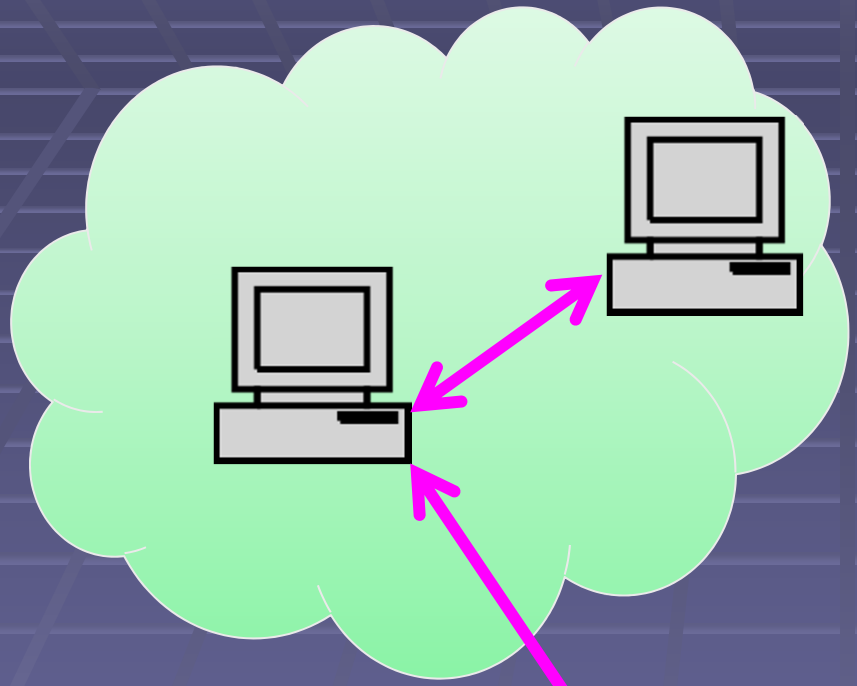




У меня было 3 яблока.
Мне дали еще 2.
Сколько у меня теперь яблок?

Алиса

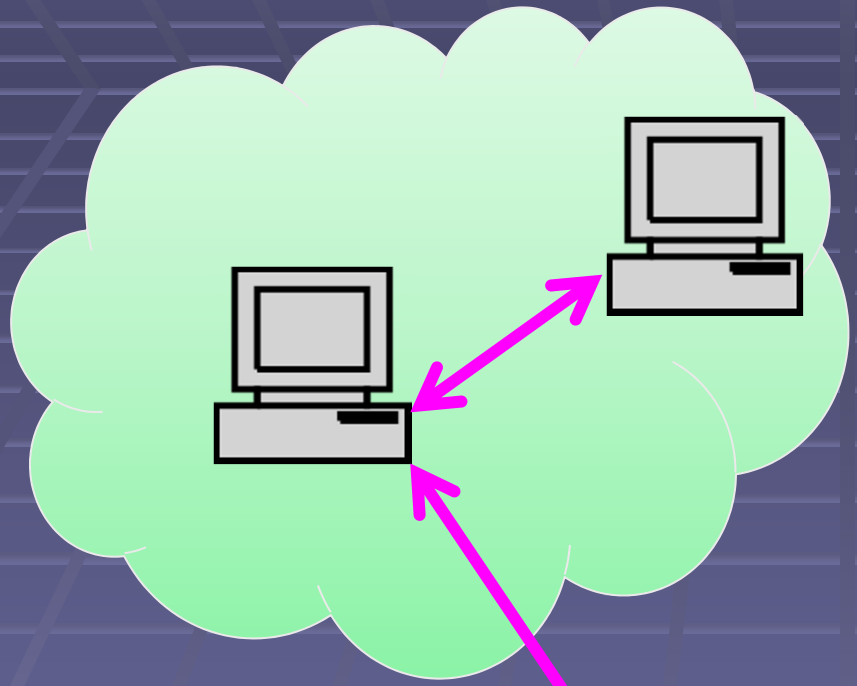
Облачные вычисления



3+2=?

Алиса

Облачные вычисления



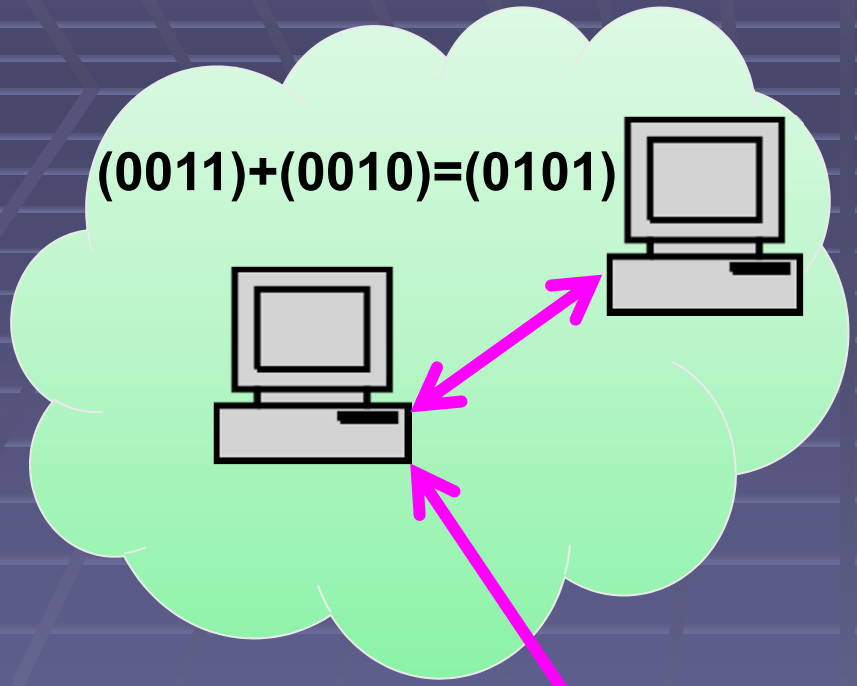
$(0011)_2+(0010)_2$

Алиса

$3=(0011)_2$

$2=(0010)_2$

Облачные вычисления



$(0011)_2+(0010)_2$

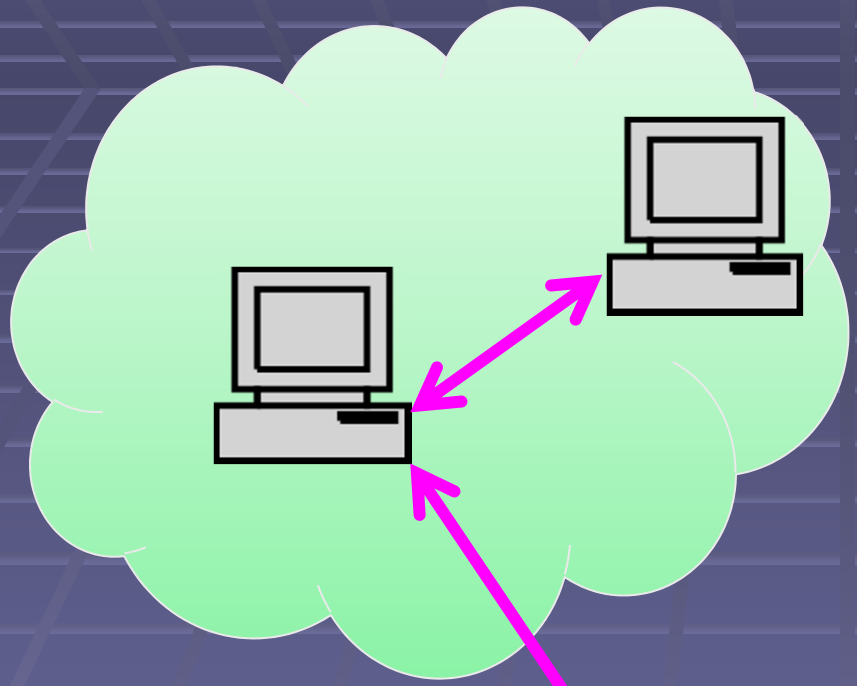
Алиса

(0011)+(0010)=(0101)

Гарри,
злоумышленник

Вот это да!
У Алисы 5 яблок!
Пойду к ней в гости.

Облачные вычисления



В облачных вычислениях данные нужно защищать. ЗАШИФРУЕМ ДАННЫЕ!!!

Алиса

Криптосистема с секретным ключом

m – открытый текст – данные,

k – секретный ключ – случайное число,

E – шифратор – алгоритм шифрования,

D – дешифратор – алгоритм расшифрования

c=E(m,k) – шифртекст – зашифрованные данные,

D(c,k)=m

Криптосистема с секретным ключом

SCC = (M, C, K, P, E, D)

M – пространство открытых текстов,

C – пространство шифртекстов,

K – пространство ключей,

$P : \rightarrow K$ – алгоритм выбора ключей,

$E: M \times K \rightarrow C$ – шифратор,

$D: C \times K \rightarrow M$ – дешифратор.

Шифр Вернама

m: (0011), (0010)

k: (10100110) - случайная двоичная строка

E: c = m ⊕ k

m: 0 0 1 1 0 0 1 0

⊕

k: 1 0 1 0 0 1 1 0

c: 1 0 0 1 0 1 0 0

D: m = c ⊕ k

c: 1 0 0 1 0 1 0 0

⊕

k: 1 0 1 0 0 1 1 0

m: 0 0 1 1 0 0 1 0

D(E(m,k),k)=m

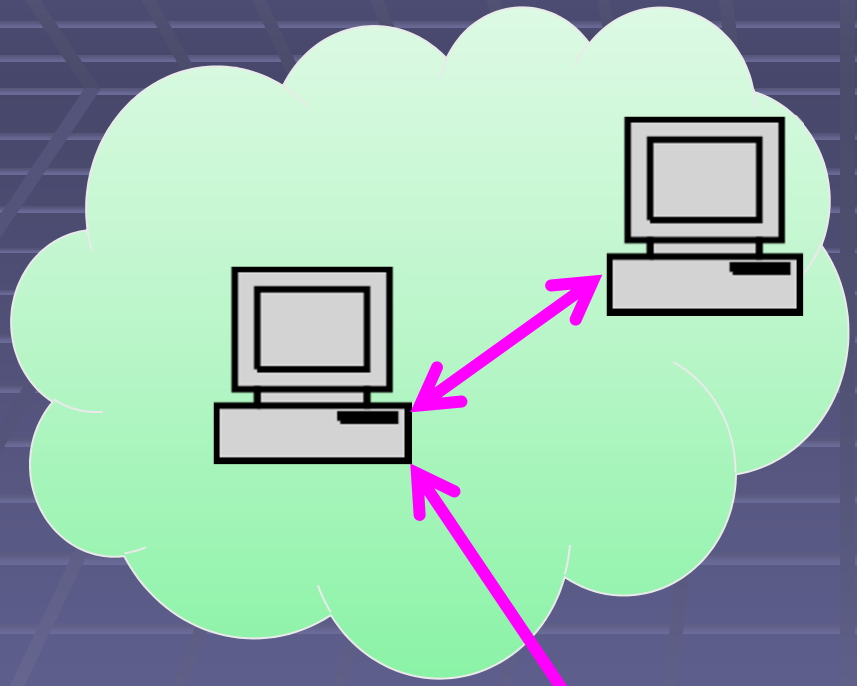
Шифр Вернама

А почему эта криптосистема стойкая?

m_1:	11111111	m_2:	01010101	m_3:	0000000
	⊕		⊕		⊕
k_1:	10100110	k_2:	00001100	k_3:	01011001
c:	01011001		01011001		01011001

Без секретного ключа, из шифртекста нельзя извлечь никакой информации об исходном сообщении.

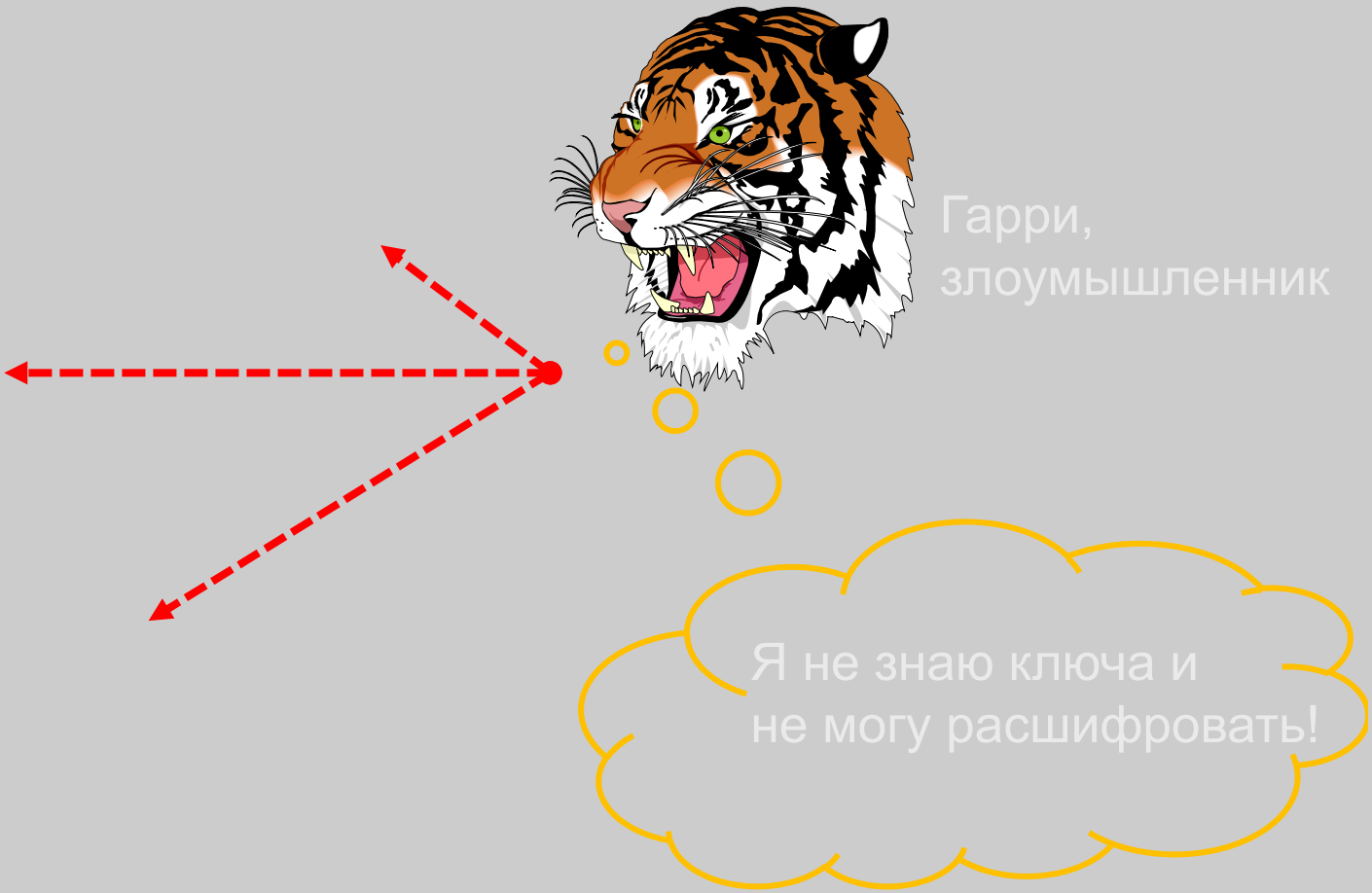
Облачные вычисления



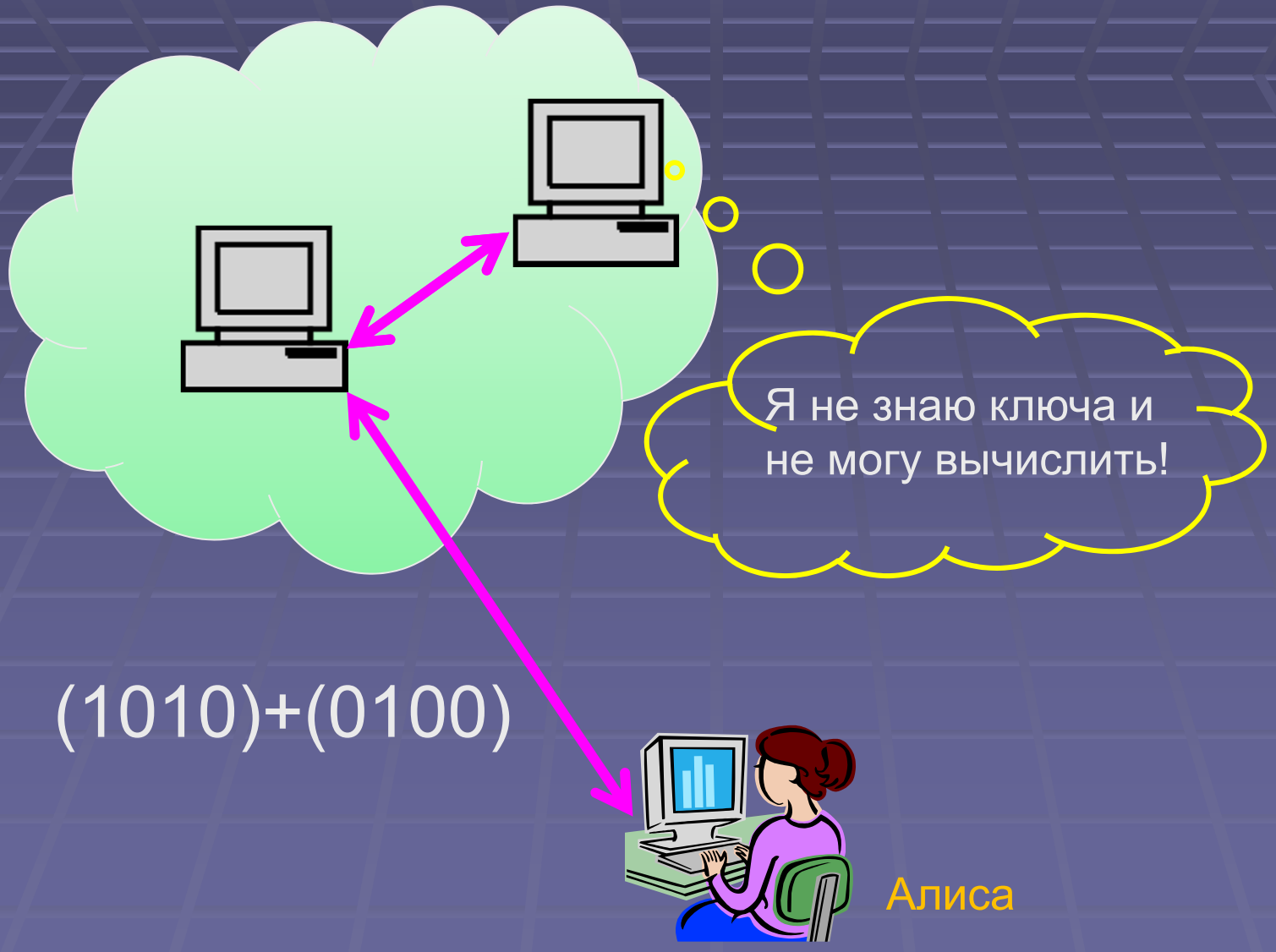
c_1+c_2
(1010)+(0100)

Алиса

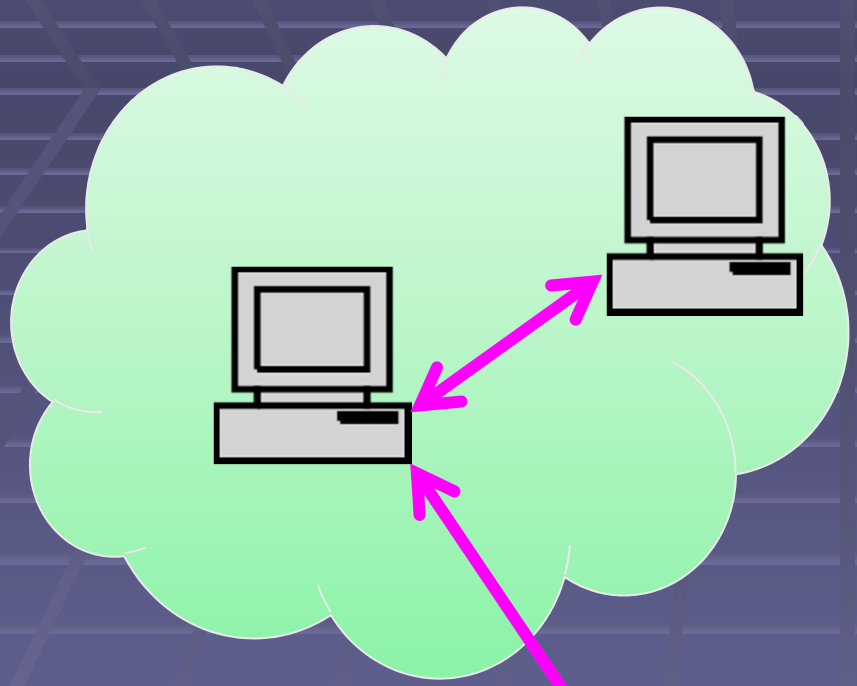
$c_1=E(3,k)=(1010)$
$c_2=E(2,k)=(0100)$


Гарри,
злоумышленник
Я не знаю ключа и
не могу расшифровать!

Облачные вычисления



Облачные вычисления



Шифровать надо так, чтобы над шифртекстами можно было проводить вычисления!!!

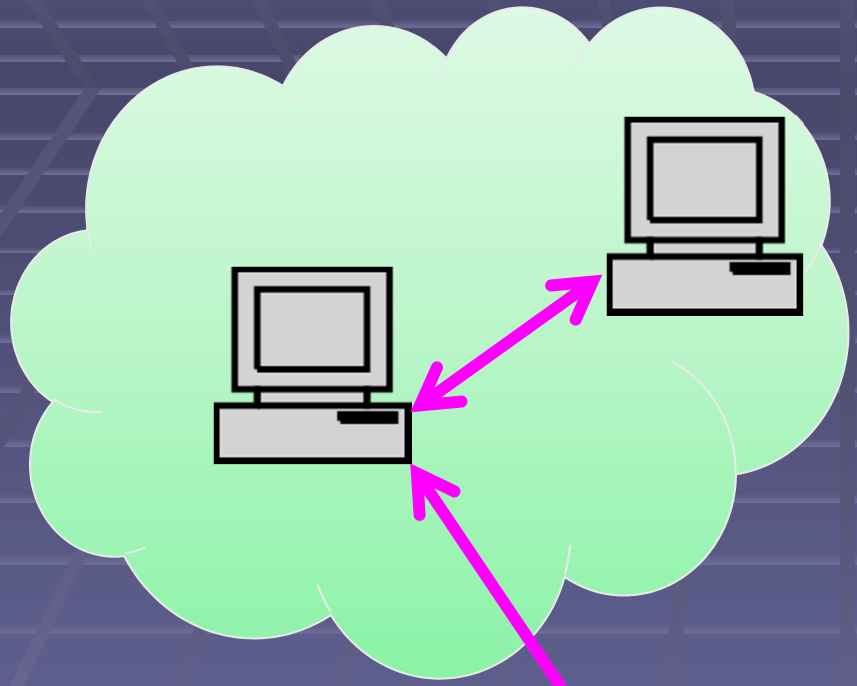
Алиса

Гомоморфное шифрование

Предположим, что на множестве M открытых текстов определена некоторая операция $\bullet$ (например, операция $+$ на множестве целых чисел), и на множестве шифртекстов C определена операция $\otimes$. Тогда криптосистема (M,C,K,P,E,D) осуществляет гомоморфное шифрование (относительно операции $\bullet$), если выполняется условие

$$E(m_1 \bullet m_2, k) = E(m_1,k) \otimes E(m_2,k)$$

Облачные вычисления



Мне нужна криптосистема, гомоморфная относительно сложения натуральных чисел!

Алиса

Криптосистема с открытым ключом

m – открытый текст – данные,

ks – секретный ключ (для расшифрования)

kp – открытый ключ (для шифрования)

E – шифратор – алгоритм шифрования,

D – дешифратор – алгоритм расшифрования

c=E(m, kp) – шифртекст – зашифрованные данные,

D(c, ks)=m

Криптосистема Эль-Гамаля

1. Генерация ключей

а). Выберите простое число q (например, 37)

б). Выберите простое число $g : g<q$
(например, 19)

в). Выберите случайное число $x : 1<x<q-1$
(например, 5)

д). Вычислите $h=g^x \bmod q$
(в нашем случае, $19^5 \bmod 37=22$)

Открытый ключ: kp=(q,g,h) (у нас: (37,19, 22))

Секретный ключ: ks=x (у нас: 5)

Криптосистема Эль-Гамаля

2. Шифрование с ключом kp=(q,g,h)

Чтобы зашифровать число m (например, 3)

а). Выберите случайное число $y : 1<y<q-1$

(например, 12)

б). Вычислите $c_1=g^y \bmod q$ и $c_2=m \cdot h^y \bmod q$

(в нашем случае, $c_1=10$ и $c_2=4$)

Тогда шифр числа m : E(m,kp)=(c_1, c_2)

(в нашем случае шифр числа 3 : (*10, 4*)

Криптосистема Эль-Гамаля

3. Расшифрование с ключом ks=x

Чтобы расшифровать криптограмму (c_1, c_2)
(в нашем случае, (10,4))

вычислите

$$m = D((c_1, c_2), x) = c_2 \cdot c_1^{q-1-x} \bmod q .$$

(в нашем случае,

$4 \cdot 10^{37-1-5} \bmod 37 = 4 \cdot 10^{31} \bmod 37 =$ 3!!!)

Криптосистема Эль-Гамаля

В чем же состоит фокус?

$D((c_1, c_2),x) =$

$c_2 \cdot c_1^{q-1-x} \bmod q =$ $[c_1=g^y \bmod q,\ c_2=m \cdot h^y \bmod q]$

$m \cdot h^y \cdot (g^y)^{q-1-x} \bmod q =$ $[h= g^x]$

$m \cdot (g^x)^y \cdot (g^y)^{q-1-x} \bmod q =$

$m \cdot g^{xy + y(q-1) - yx} \bmod q =$

$m \cdot (g^{q-1})^y \bmod q =$

$[g^{q-1} \bmod q = 1$: малая теорема Ферма$]$

$m \cdot 1^y \bmod q = m$

Криптосистема Эль-Гамаля

А почему шифрование стойкое?

А потому, что решить уравнение

$$e=g^x \bmod q$$

очень трудно!

Современная математика позволяет решать такие уравнения только перебором всех возможных чисел от 0 до q-1.

Криптосистема Эль-Гамаля

гомоморфна относительно сложения

Если $E(m,kp)=(c_1, c_2)$ и $E(n,kp)=(d_1, d_2)$, то

$$E(m+n,kp)=(c_1 \times d_1 , c_2 \times d_2).$$

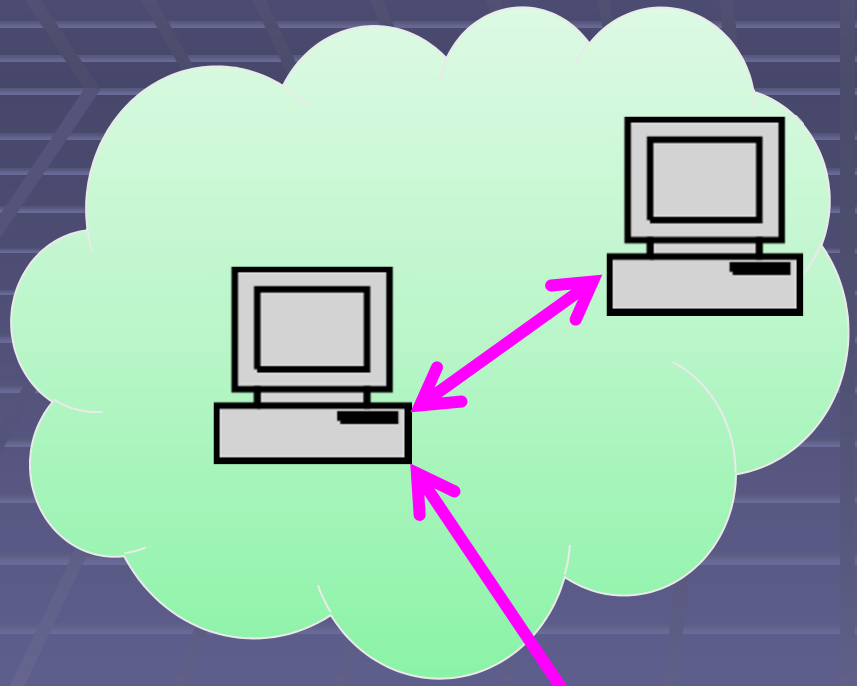
И верно, в нашем случае $E(3,kp)=(10, 4)$.

Поэтому 3+3 можно вычислить так:

$$(10, 4)\times(10, 4)=(100,16)=(26,16) \bmod 37$$

$$D((26,16), ks)= 16 \cdot 26^{37-1-5} \bmod 37 = 6 \text{ !!!}$$

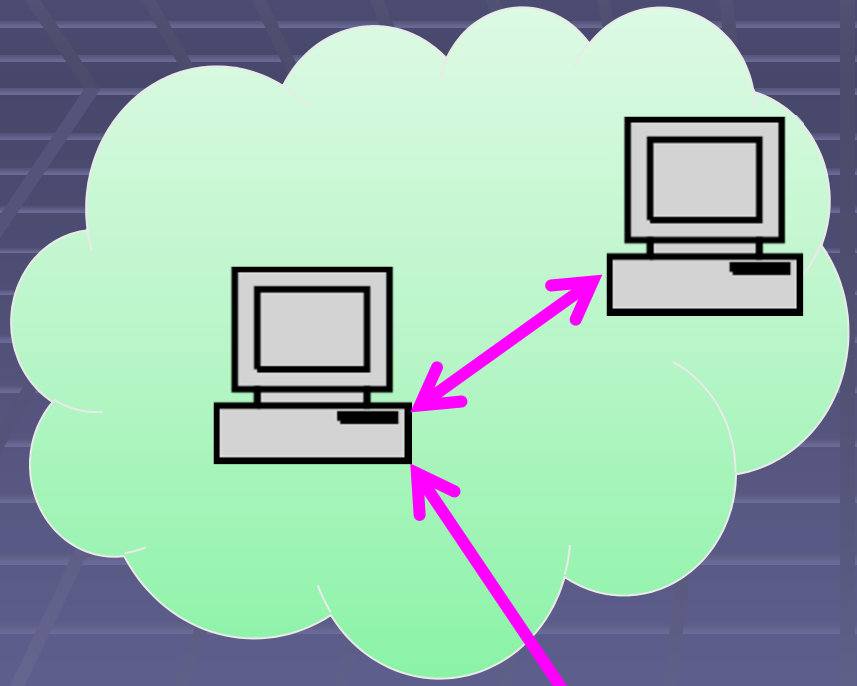
Облачные вычисления



Воспользуюсь криптосистемой Эль-Гамаля!

Алиса

Облачные вычисления

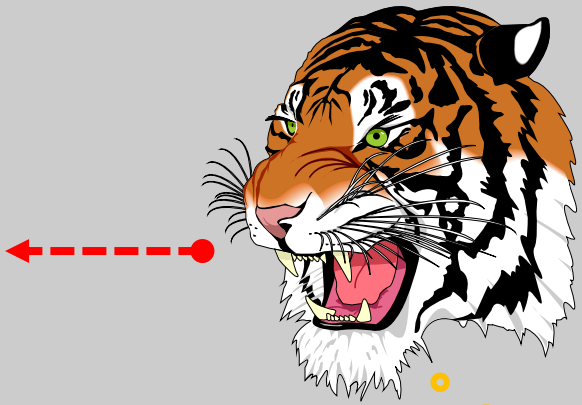


(10,4)+(10,15)

Алиса

E(3,kp)=(10,4)

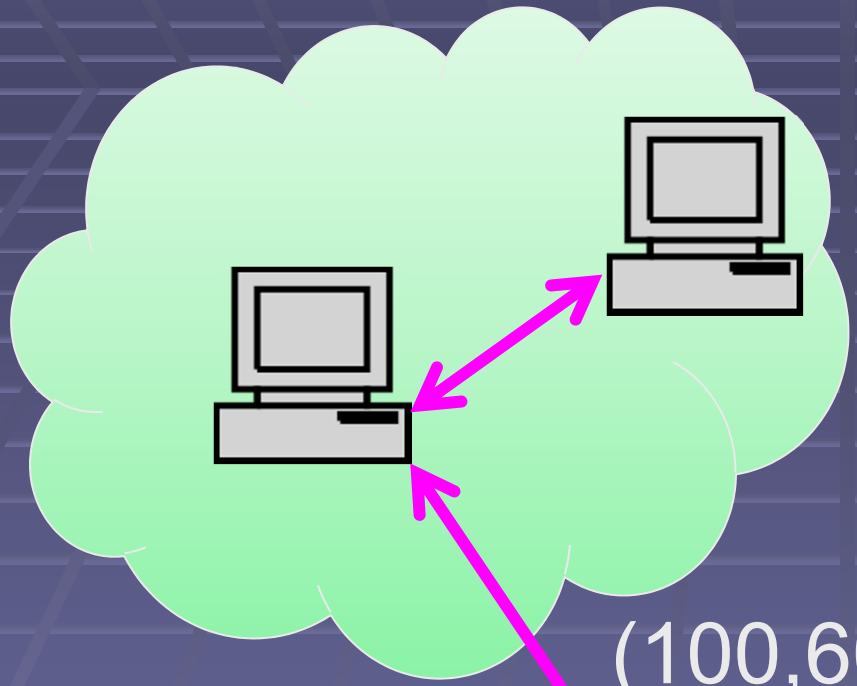
E(2,kp)=(10,15)



Гарри,
злоумышленник

Ничего не
понимаю!

Облачные вычисления

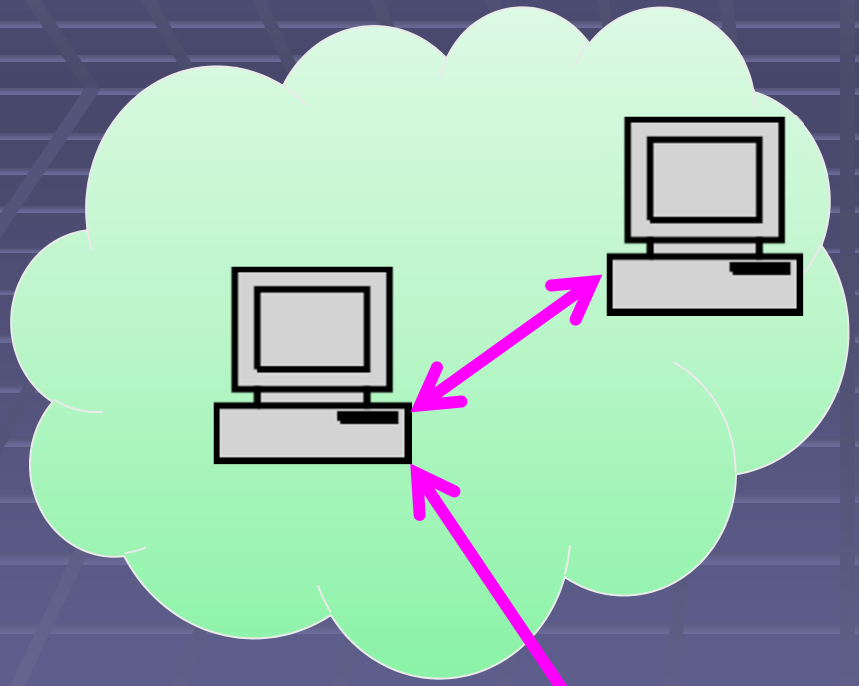


(100,60)=
=(26,23)

D((26,23),ks)=5

Алиса

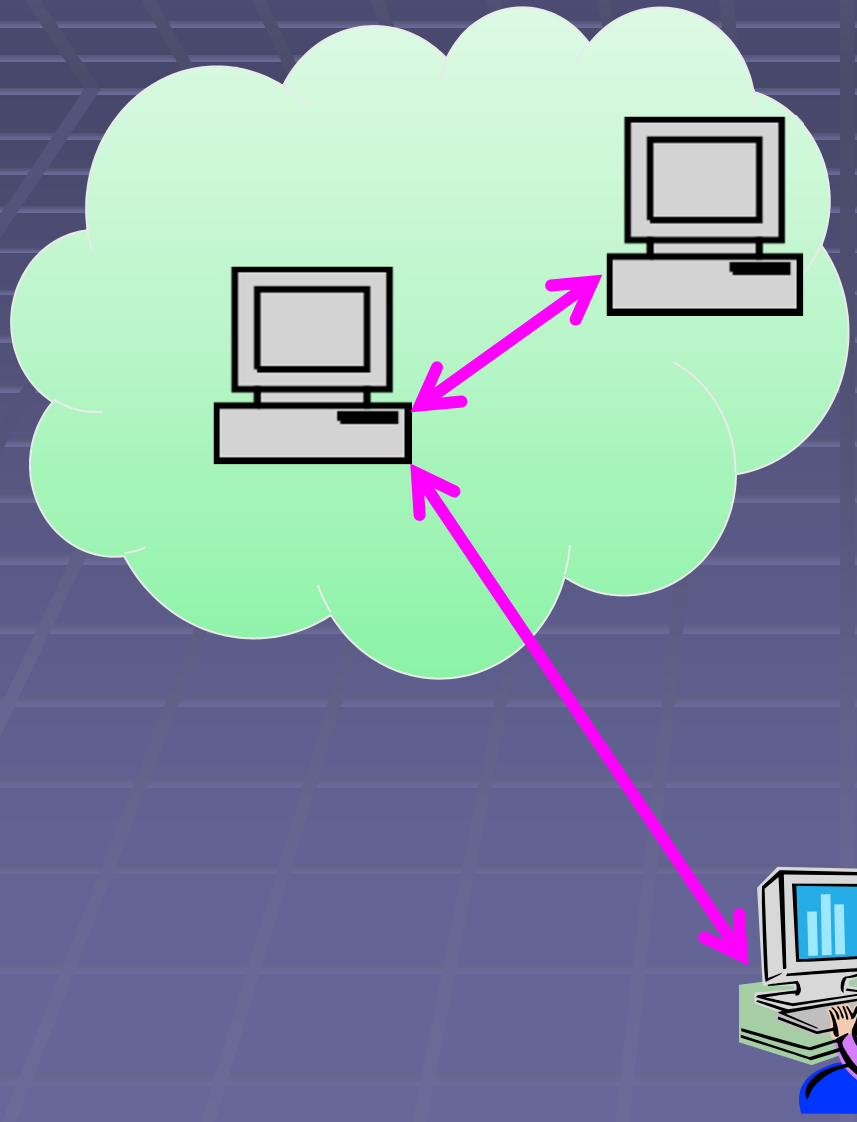
Облачные вычисления



Алиса

А если я захочу умножить 2×3 ?

Облачные вычисления



Увы, криптоситема Эль-Гамаля не является гомоморфной относительно умножения!

Алиса

Гомоморфное шифрование

Криптосистема,
осуществляющая шифрование 0 и 1
и
являющаяся при этом гомоморфной относительно сложения и умножения по модулю 2,
называется вполне гомоморфной криптосистемой.

Вполне гомоморфное шифрование

Впервые стойкую систему
вполне гомоморфного шифрования
разработал
Крейг Джентри (Craig Gentry, MIT)
в 2009 г.

Вполне гомоморфное шифрование

Генерация ключа: выберите произвольное нечетное число p

Шифрование бита m:

- выберите достаточно большое число q и небольшое число r ,
- вычислите $c = pq + 2r + m$.

Расшифрование шифртекста c:

- вычислите $m = (c \bmod p) \bmod 2$.

Вполне гомоморфное шифрование

Допустим, что $c_1=q_1p+2r_1+m_1$, $c_2=q_2p+2r_2+m_2$

Тогда $c_1+c_2 = (q_1+q_2)p + 2(r_1+r_2) + (m_1+m_2)$

и если $2(r_1+r_2)+(m_1+m_2)$ гораздо меньше p, то

$D(E(m_1) + E(m_2)) = (c_1+c_2 \bmod p) \bmod 2 =$

$(2(r_1+r_2) + (m_1+m_2)) \bmod 2 =$

$m_1+m_2 \bmod 2$

Таким образом, $D(E(m_1)+ E(m_2)) = m_1+m_2$

Вполне гомоморфное шифрование

Допустим, что $c_1=q_1p+2r_1+m_1$, $c_2=q_2p+2r_2+m_2$

Тогда $c_1 \times c_2 = (c_1q_2+q_1c_2-q_1q_2)p + 2(2r_1r_2+r_1m_2+m_1r_2) + m_1m_2$

и если $2(2r_1r_2+r_1m_2+m_1r_2)$ гораздо меньше p, то

$D(E(m_1) \times E(m_2)) = (c_1 \times c_2 \bmod p) \bmod 2 =$

$(2(2r_1r_2+r_1m_2+m_1r_2) + m_1m_2) \bmod 2 =$

$m_1 \times m_2$

Таким образом, $D(E(m_1) \times E(m_2)) = m_1 \times m_2$

Вполне гомоморфное шифрование

Генерация ключа: выбираем $p=99$

Шифрование двух битов *1*:

выбираем $q_1=37$ и $q_2=82$, *а также* $r_1=3$, и $r_2=2$.

вычисляем $c_1 = q_1p+2r_1+1=3670$, $c_2 =q_2p+2r_2+1=8123$.

Вычисление суммы $1 \oplus 1$ и произведения 1×1:

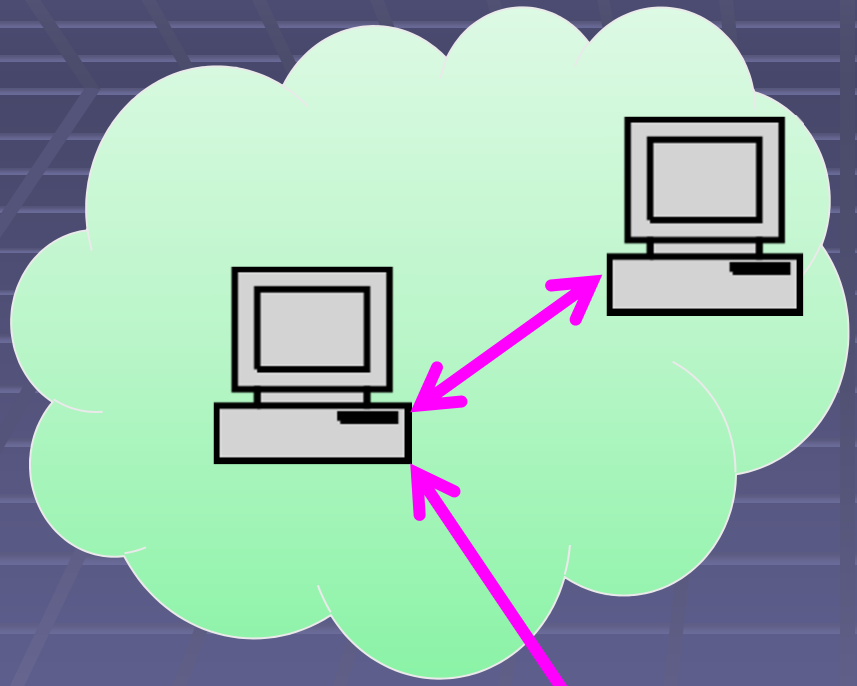
$c_1 + c_2 = 11793$, $c_1 \times c_2 = 29811410$

Расшифрование результата:

$(11793 \bmod 99) \bmod 2 = 4 \bmod 2 = 0 = 1 \oplus 1$

$(9032270 \bmod 99) \bmod 2 = 35 \bmod 2 = 1 = 1 \times 1$.

Облачные вычисления



Неужели все так просто ?

Алиса

Трудности вполне гомоморфного шифрования

Нельзя вычислять очень долго с одним и тем же ключом p.

$$c_1 \times c_2 = (c_1 q_2 + q_1 c_2 - q_1 q_2)p + 2(2r_1 r_2 + r_1 m_2 + m_1 r_2) + m_1 m_2$$

Если $2(2r_1 r_2 + r_1 m_2 + m_1 r_2) > p/2$, то

$$D(E(m_1) \times E(m_2)) \neq m_1 \times m_2$$

Что же делать ?

Трудности вполне гомоморфного шифрования

Нужно постоянно перешифровывать данные на новом ключе. И это можно делать секретно. От шифра $E(m,p_1)$ к шифру $E(m,p_2)$ можно перейти

1) вычислив над шифром $E(m,p_1)$ функцию

$E(D(E(m,p_1), p_1), p_2)$ и получив в результате шифр $E(E(m,p_2),p_1)$,

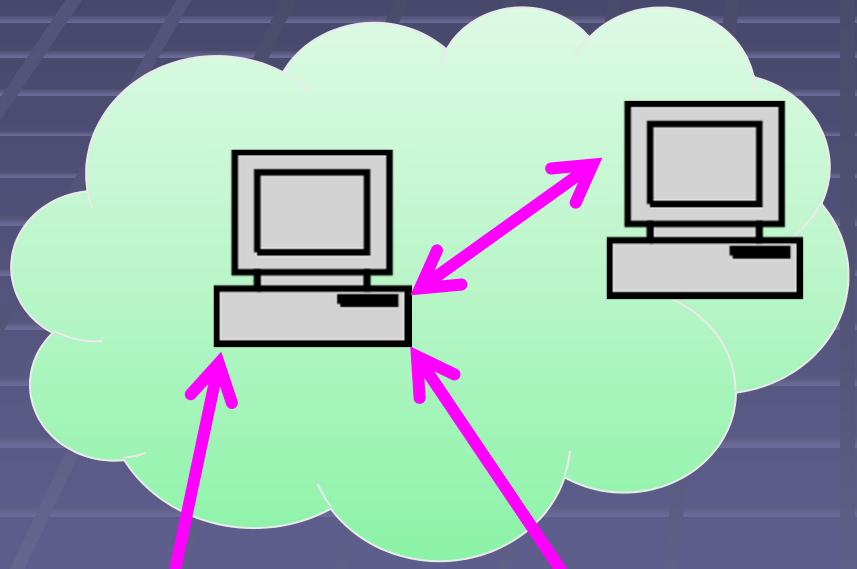
2) расшифровав результат

$$E(m,p_2)=D(E(E(m,p_2),p_1),p_1).$$

Трудности вполне гомоморфного шифрования

Эта операция называется «перезагрузка» (bootstrapping). Она очень сильно замедляет вычисления. Поэтому пока гомоморфные криптосистемы строятся и изучаются только в «лабораторных» условиях.

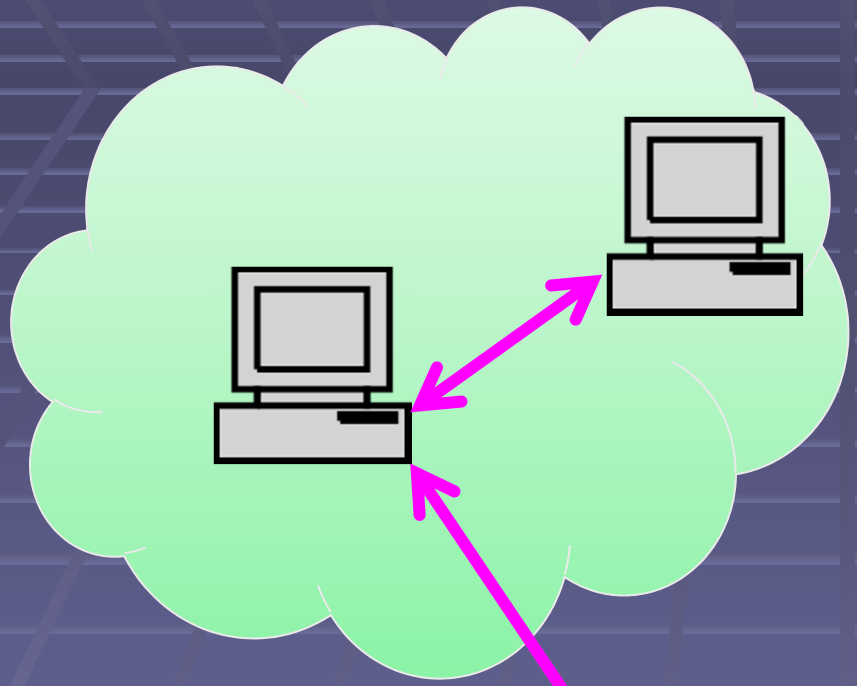
Трудности вполне гомоморфного шифрования



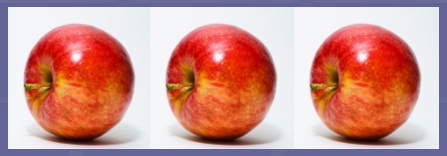
В более общих случаях одного лишь свойства гомоморфизма уже недостаточно!

Боб

Алиса



Может быть, скоро гомоморфное шифрование станет более практичным, и я смогу вычислить, сколько у меня яблок. До встречи, друзья.



Алиса

СПАСИБО

ЗА

ВНИМАНИЕ