

Криптография -1

Виталий Павленко
CTF на Физтехе

Темы

- Кодировки
- Классические шифры
- Одноразовый блокнот
- Асимметричное шифрование
- Хеширование

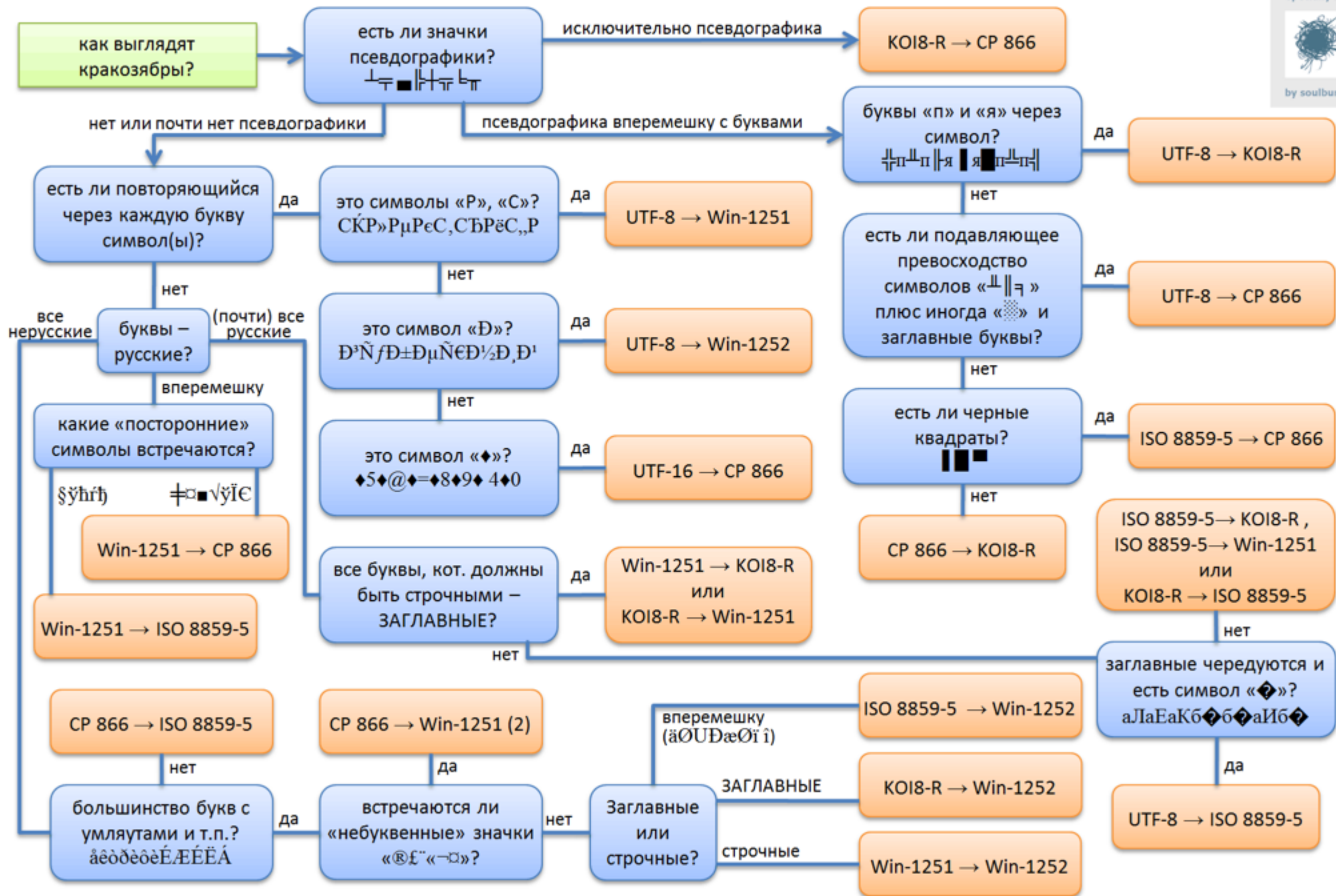
Философия: что делать руками?

- Сортировка чисел и строк
- Разложение на простые множители
- Перевод из одной кодировки в другую
- Перевод азбуки Морзе в буквы
- Поиск и замена в тексте

Делайте то, что нетривиально

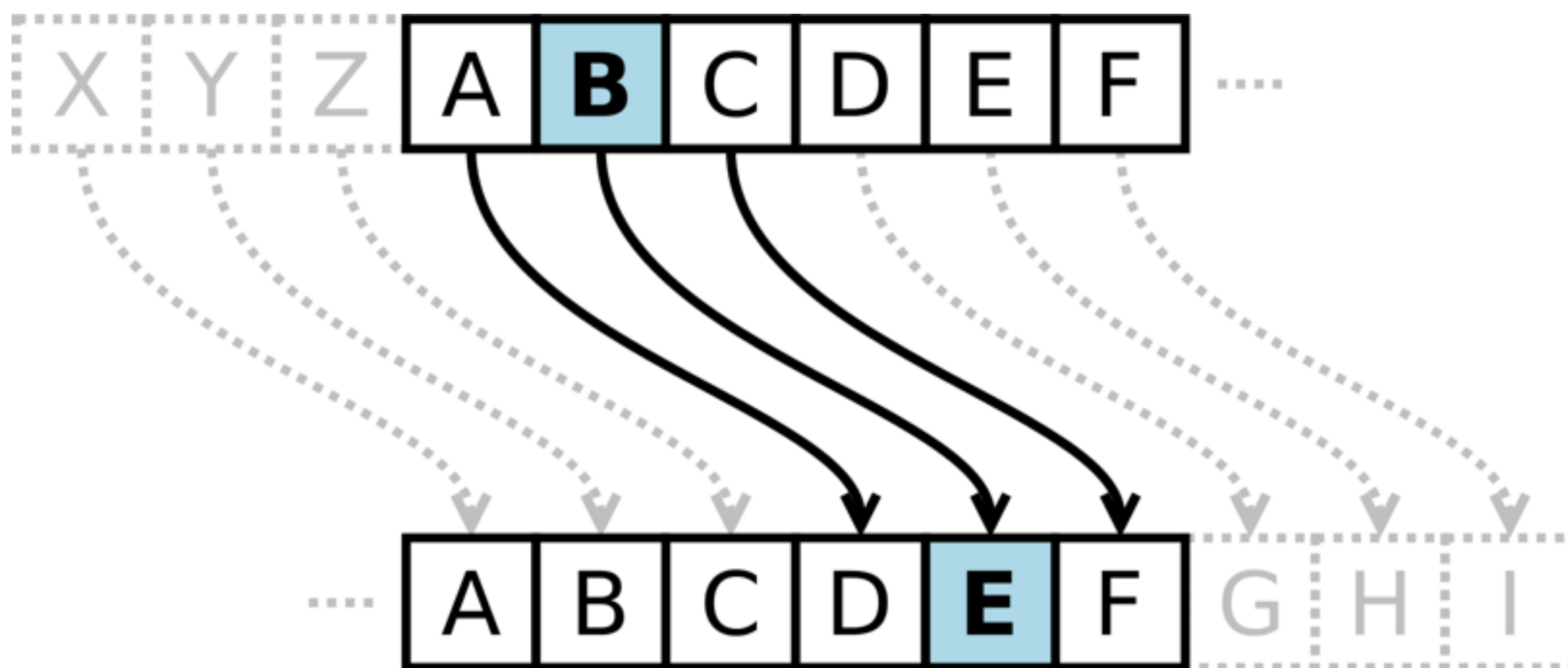
- Умеет ли это делать ваш текстовый редактор?
- Есть ли консольная утилита, которая это делает?
- Можно ли нагуглить веб-инструмент для решения этой задачи?
- Можно ли найти исходный код программы, которая это делает?
- Пишите утилиту сами, только если по всем прочим пунктам — «нет»

Кодировки



Классические шифры

Шифр Цезаря

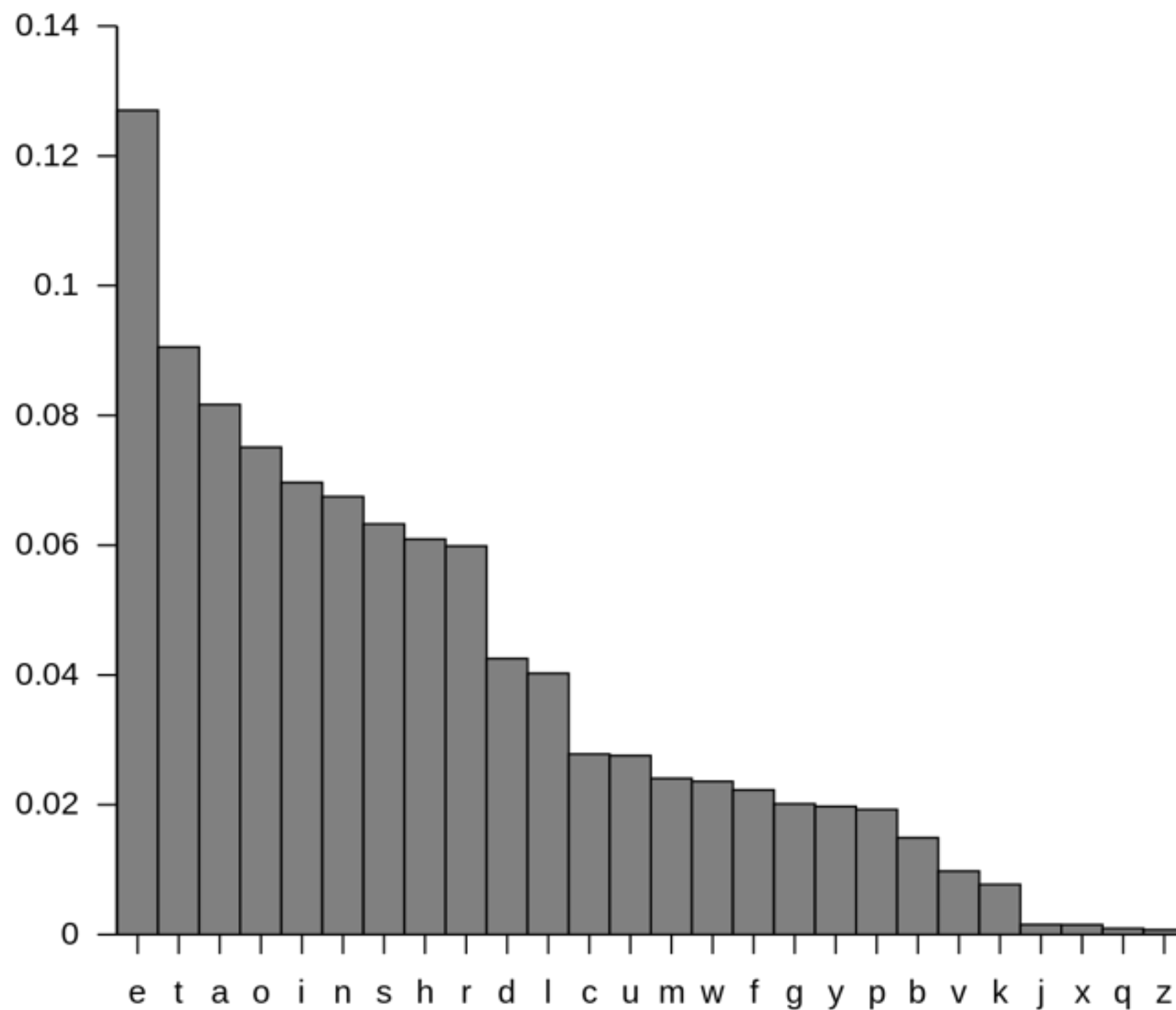


Шифр подстановки

💣😬⊕💀✈️ ✕👉💧 😊 🙌😊💣🙌😬👉👉 ✈️☾😊🙌🙌🙌
😊 ⚙️👉👉✕ ⚙️💣😊🙌💀✕ 💧☾😊💧 ✈️💧✕👉💧✈️
😊🙌🙌 ⊕✕💀💧✈️ ☾😊✈️ ☾👉👉✕ 👉⚙️👉👉 💧☾💀
✈️💧😊👉💀 😊🙌🙌 💧☾💀👉 😬✈️ ☾💀😊✕🙌 🙌🙌
✕👉✕💀 😬💧 😬✈️ 😊 💧😊💣💀 💧👉💣🙌 ✕🙌
😊👉 😬🙌😊👉💧 ⊕👉💣💣 🙌⊕ ✈️👉👉🙌🙌 😊🙌🙌
⊕👉✕🙌 ✈️😊👉👉😊⊕🙌😊👉👉 🙌🙌💧☾😊👉👉

(Click to make larger)

Частотный анализ



Шифр Виженера

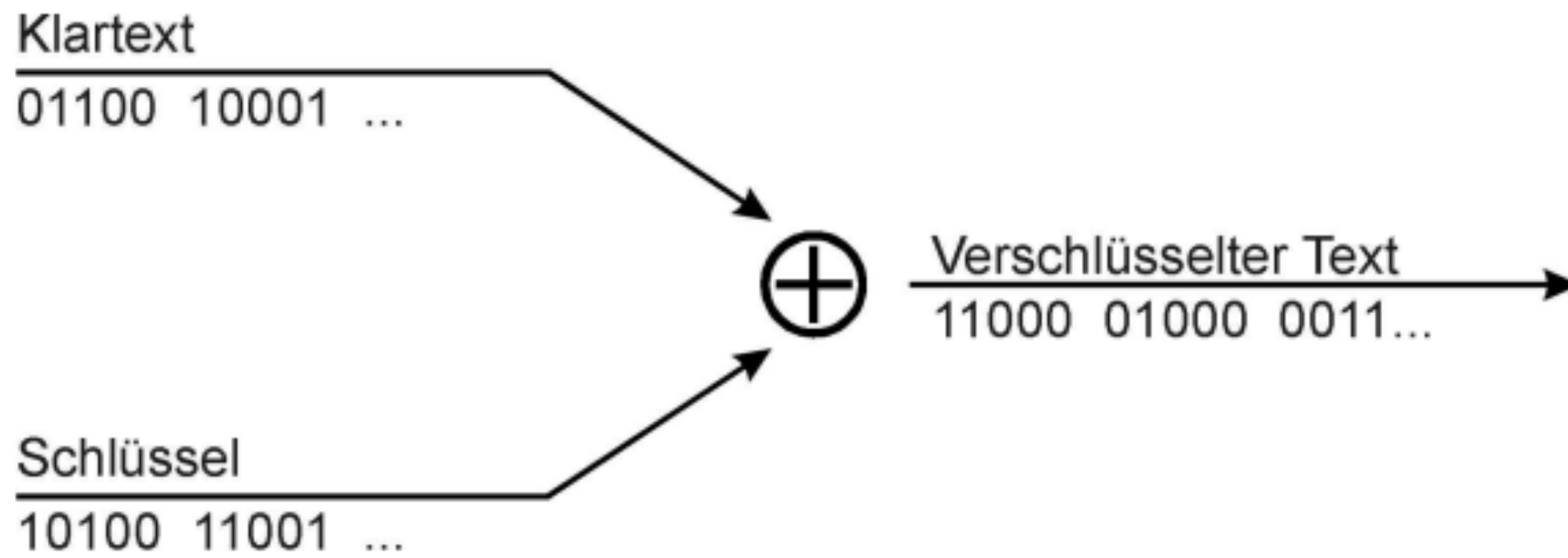
Ключ	<u>A</u>	<u>B</u>	<u>C</u>	<u>D</u>	<u>E</u>	<u>F</u>	<u>G</u>	<u>H</u>	<u>I</u>	<u>J</u>	<u>K</u>	<u>L</u>	<u>M</u>	<u>N</u>	<u>O</u>	<u>P</u>	<u>Q</u>	<u>R</u>	<u>S</u>	<u>T</u>	<u>U</u>	<u>V</u>	<u>W</u>	<u>X</u>	<u>Y</u>	<u>Z</u>
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

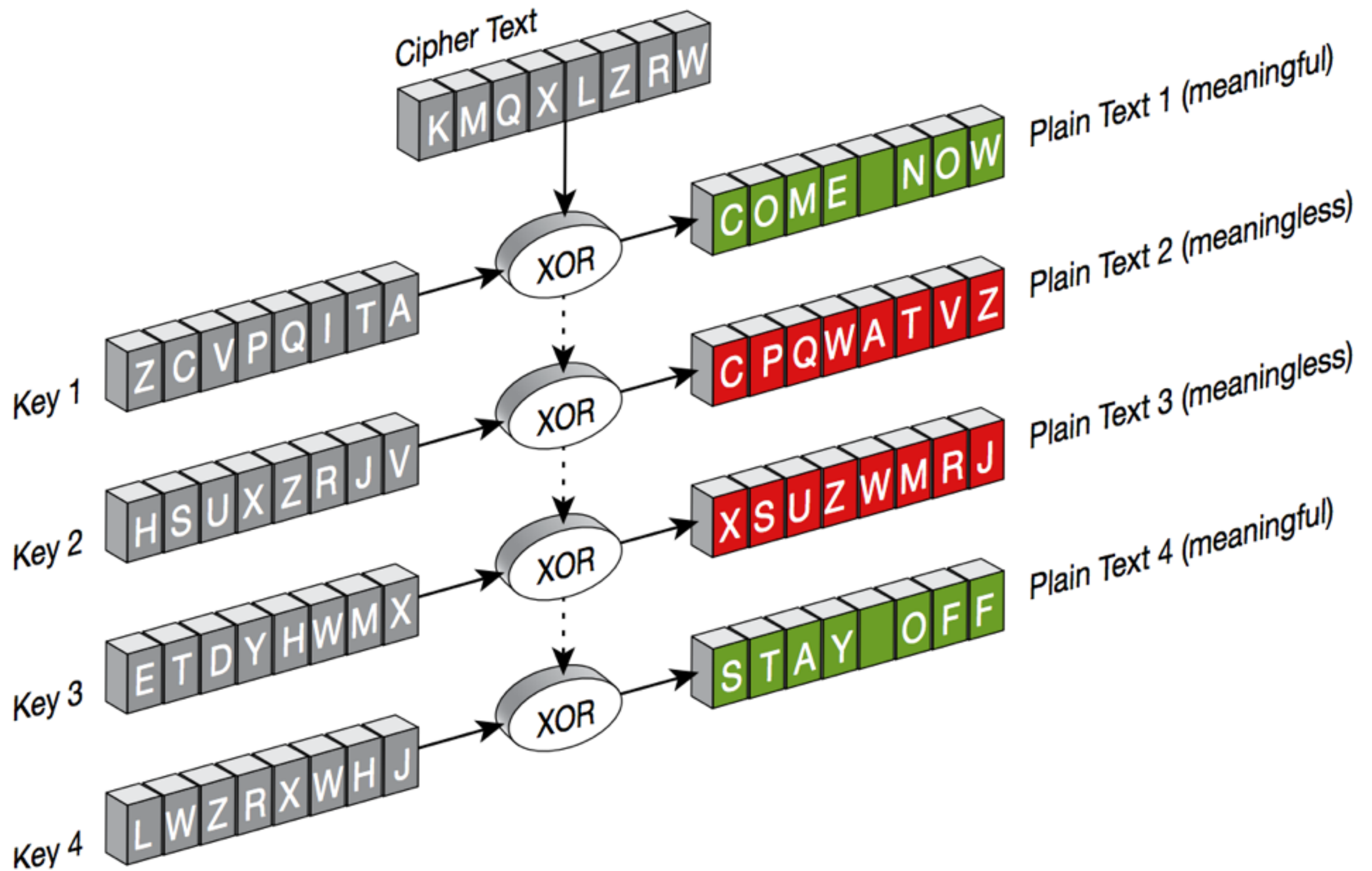
Открытый текст : GOD IS ON OUR SIDE
LONG LIVE THE KING

Ключ : PRO PA GA NDA PROP AGAN
DAPR OPA GAND

зашифрованный текст: VFR XS UN BXR
HZRT LUNT OIKV HWE QIAJ

Одноразовый блокнот





Асимметричное шифрование

Арифметика остатков

- Зафиксируем модуль 19.
- Как быстро посчитать $2^{14} \bmod 19$?
- Чему равно $2^{18} \bmod 19$?
- Чему равно $2^{19} \bmod 19$?
- Чему равно $2^{(-1)} \bmod 19$?

Проблема дискретного логарифмирования

- Работаем в арифметике над целыми числами
- Я загадал степень k числа 2, причем $2^k = 4096$.
Чему равно k ?
- Теперь работаем в арифметике остатков по модулю 509.
- Я загадал степень k числа 2, причем $2^k = 94$.
Чему равно k ?

Fermat's Little Theorem

If p is a prime and a is any integer, then $a^p \equiv a \pmod{p}$.

Definition

The **Euler φ -Function** is defined on the set of positive integers as follows. For each positive integer n , $\varphi(n)$ is the number of integers a satisfying $1 \leq a \leq n$ and $(a, n) = 1$.

Recall: The group of units of the ring \mathbb{Z}_n of integers mod n is

$$\mathbb{Z}_n^* = \{[a]_n \mid 1 \leq a \leq n \text{ and } (a, n) = 1\},$$

hence $|\mathbb{Z}_n^*| = \varphi(n)$.

Euler's Theorem

If n is a positive integer and a is any integer such that $(a, n) = 1$, then

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Протокол Диффи-Хеллмана

Alice

Bob

Choose random private key

$$k_{prA}=a \in \{1,2,\dots,p-1\}$$

Choose random private key

$$k_{prB}=b \in \{1,2,\dots,p-1\}$$

Compute corresponding public key

$$k_{pubA}=A = \alpha^a \bmod p$$

A

Compute corresponding public key

$$k_{pubB}=B = \alpha^b \bmod p$$

B

Compute common secret

$$k_{AB} = B^a = (\alpha^a)^b \bmod p$$

Compute common secret

$$k_{AB} = A^b = (\alpha^b)^a \bmod p$$

Пример

Domain parameters $p=29$, $\alpha=2$

Alice

Bob

Choose random private key

$$k_{prA} = a = 5$$

Choose random private key

$$k_{prB} = b = 12$$

Compute corresponding public key

$$k_{pubA} = A = 2^5 = 3 \bmod 29$$

A



B



Compute corresponding public key

$$k_{pubB} = B = 2^{12} = 7 \bmod 29$$


Compute common secret

$$k_{AB} = B^a = 7^5 = 16 \bmod 29$$

Compute common secret

$$k_{AB} = A^b = 3^{12} = 16 \bmod 29$$

RSA

- Pick two large primes p and q
 - Calculate $n = pq$
 - Pick e such that it is relatively prime to $\phi(n) = (q-1)(p-1)$
 - “Euler’s Totient Function”
 - $d \equiv e^{-1} \pmod{\phi(n)}$
 - or
 - $de \pmod{\phi(n)} = 1$
- 
1. $p=3, q=11$
 2. $n = 3 \cdot 11 = 33$
 3. $\phi(n) = (2 \cdot 10) = 20$
 4. $e = 7 \mid \text{GCD}(20, 7) = 1$
“Euclid’s Algorithm”
 5. $d = 7^{-1} \pmod{20}$
 $d = 7 \pmod{20} = 1$
 $d = 3$

Хеши

Замечание: Все используемые переменные 32 бита.

Инициализация переменных:

`h0 = 0x67452301`

`h1 = 0xEFCDAB89`

`h2 = 0x98BADCFE`

`h3 = 0x10325476`

`h4 = 0xC3D2E1F0`

Предварительная обработка:

Присоединяем бит '1' к сообщению

Присоединяем `k` битов '0', где `k` наименьшее число ≥ 0 такое, что длина получившегося сообщения (в битах) **сравнима по модулю** 512 с 448 (`length mod 512 == 448`)

Добавляем длину исходного сообщения (до предварительной обработки) как целое 64-битное

Big-endian число, в битах.

В процессе сообщение разбивается последовательно по 512 бит:

for перебираем все такие части

разбиваем этот кусок на 16 частей, слов по 32-бита $w[i]$, $0 \leq i \leq 15$

16 слов по 32-бита дополняются до 80 32-битовых слов:

for i **from** 16 to 79

$w[i] = (w[i-3] \text{ xor } w[i-8] \text{ xor } w[i-14] \text{ xor } w[i-16])$ циклический сдвиг влево 1

Инициализация хеш-значений этой части:

$a = h0$

$b = h1$

$c = h2$

$d = h3$

$e = h4$

ОСНОВНОЙ ЦИКЛ:

```
for i from 0 to 79
    if 0 ≤ i ≤ 19 then
        f = (b and c) or ((not b) and d)
        k = 0x5A827999
    else if 20 ≤ i ≤ 39
        f = b xor c xor d
        k = 0x6ED9EBA1
    else if 40 ≤ i ≤ 59
        f = (b and c) or (b and d) or (c and d)
        k = 0x8F1BBCDC
    else if 60 ≤ i ≤ 79
        f = b xor c xor d
        k = 0xCA62C1D6

    temp = (a leftrotate 5) + f + e + k + w[i]
    e = d
    d = c
    c = b leftrotate 30
    b = a
    a = temp
```

Добавляем хеш-значение этой части к результату:

`h0 = h0 + a`

`h1 = h1 + b`

`h2 = h2 + c`

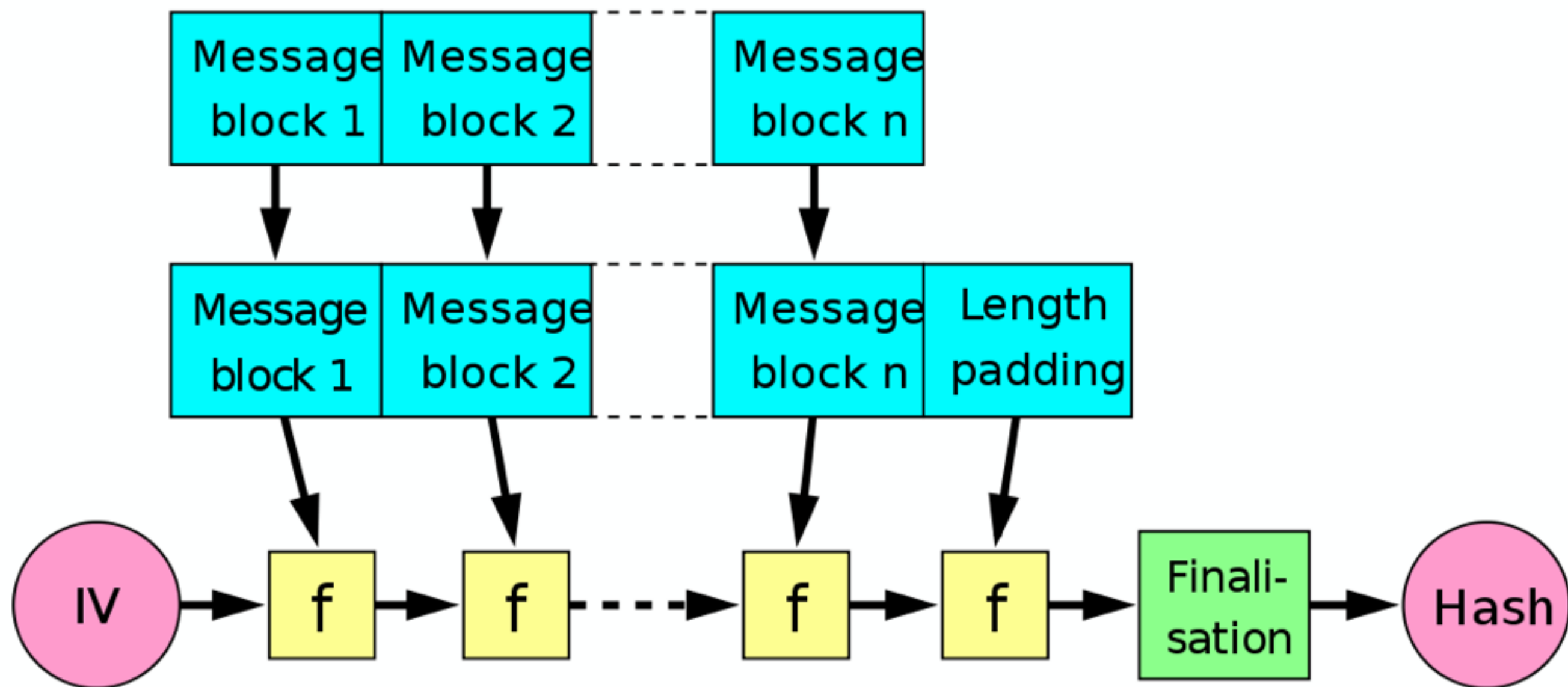
`h3 = h3 + d`

`h4 = h4 + e`

Итоговое хеш-значение:

`digest = hash = h0 append h1 append h2 append h3 append h4`

- Как сделать цифровую подпись?



Length-extension attack

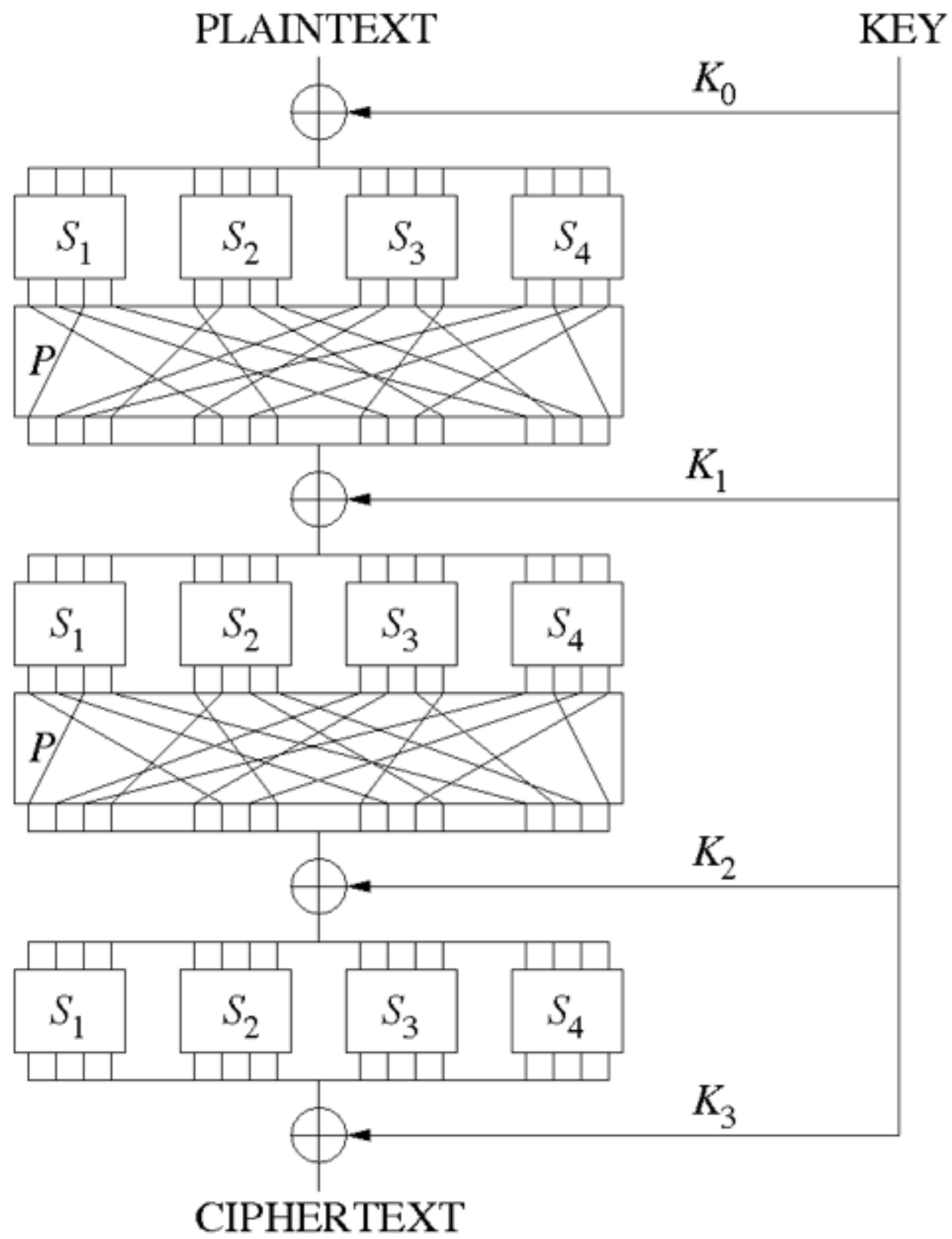
Original Data: count=10&lat=37.351&user_id=1&long=-119.827&waffle=eggo
Original Signature: 6d5f807e23db210bc254a28be2d6759a0f5f5d99

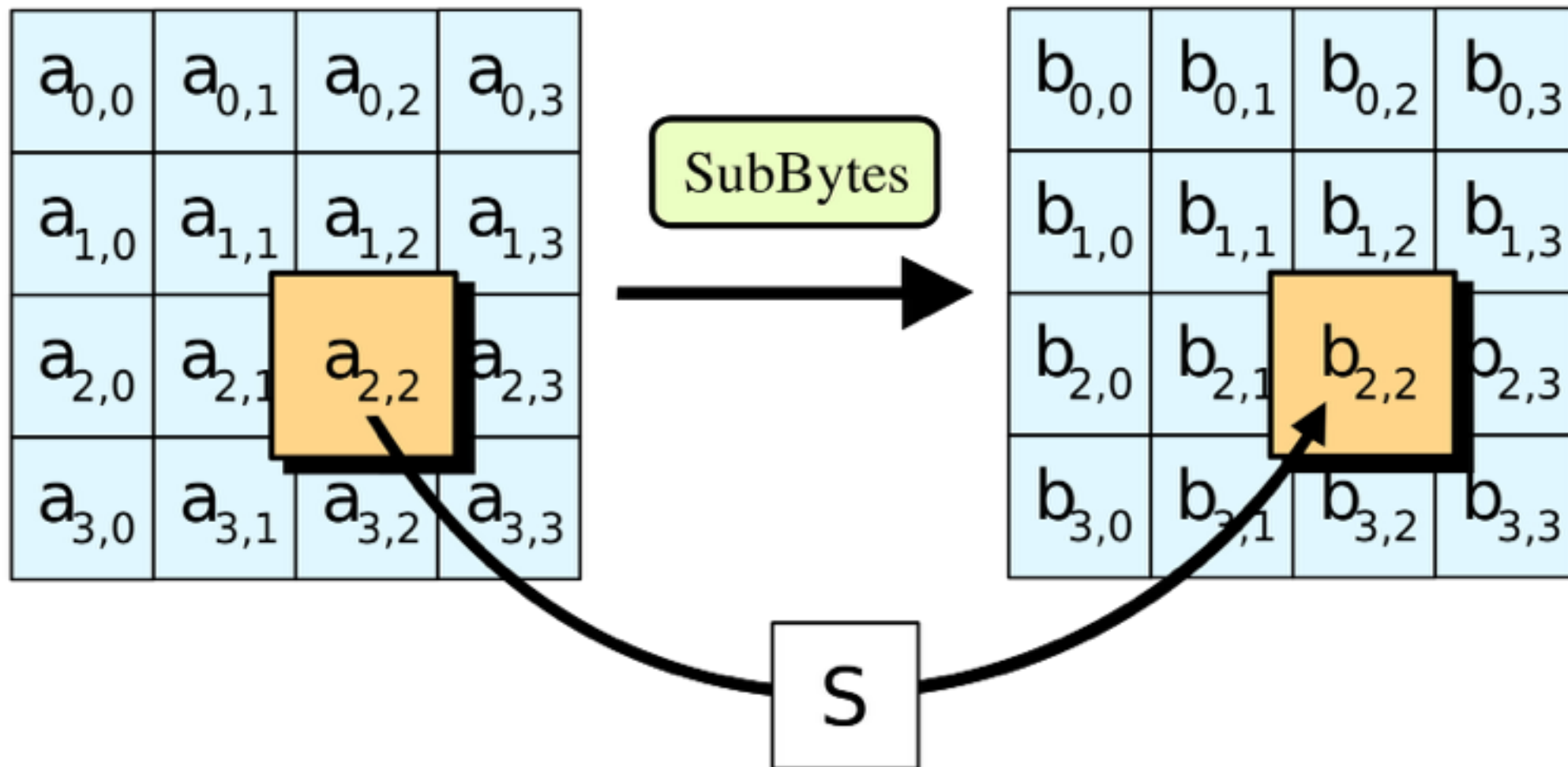
Desired New Data: count=10&lat=37.351&user_id=1&long=-119.827&waffle=eggo&waffle=liege

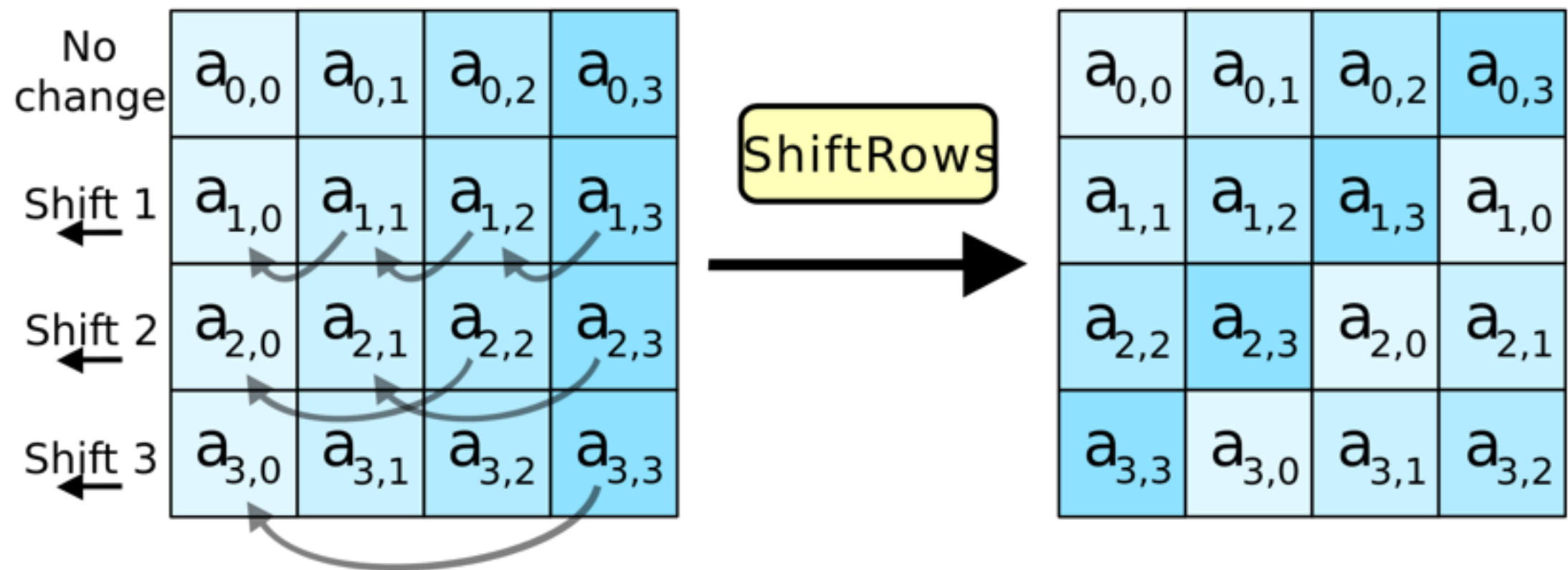
New Data: count=10&lat=37.351&user_id=1&long=-119.827&waffle=eggo\x80\x00\x00
 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
 \x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00
 \x00\x00\x00\x00\x02(&waffle=liege

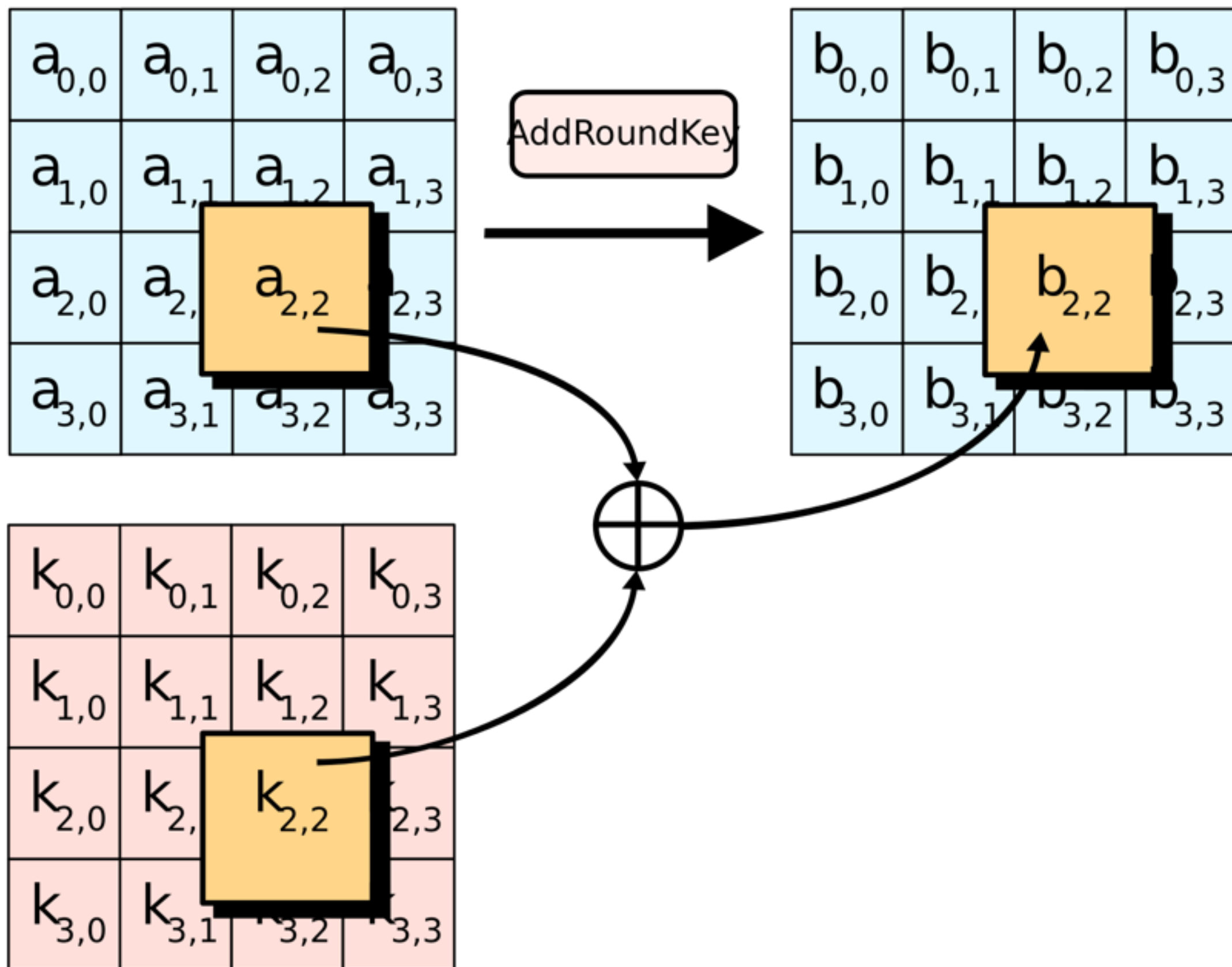
- MD5 не надёжен: люди научились находить коллизию
- fastcoll умеет генерировать два разных файла с одинаковым хэшем (содержимое вам не подвластно)
- Как сделать две таких программы: одно делает `print('Protected')`, другое `print('Cracked')`, а хэши программ одинаковые?

Симметричное шифрование

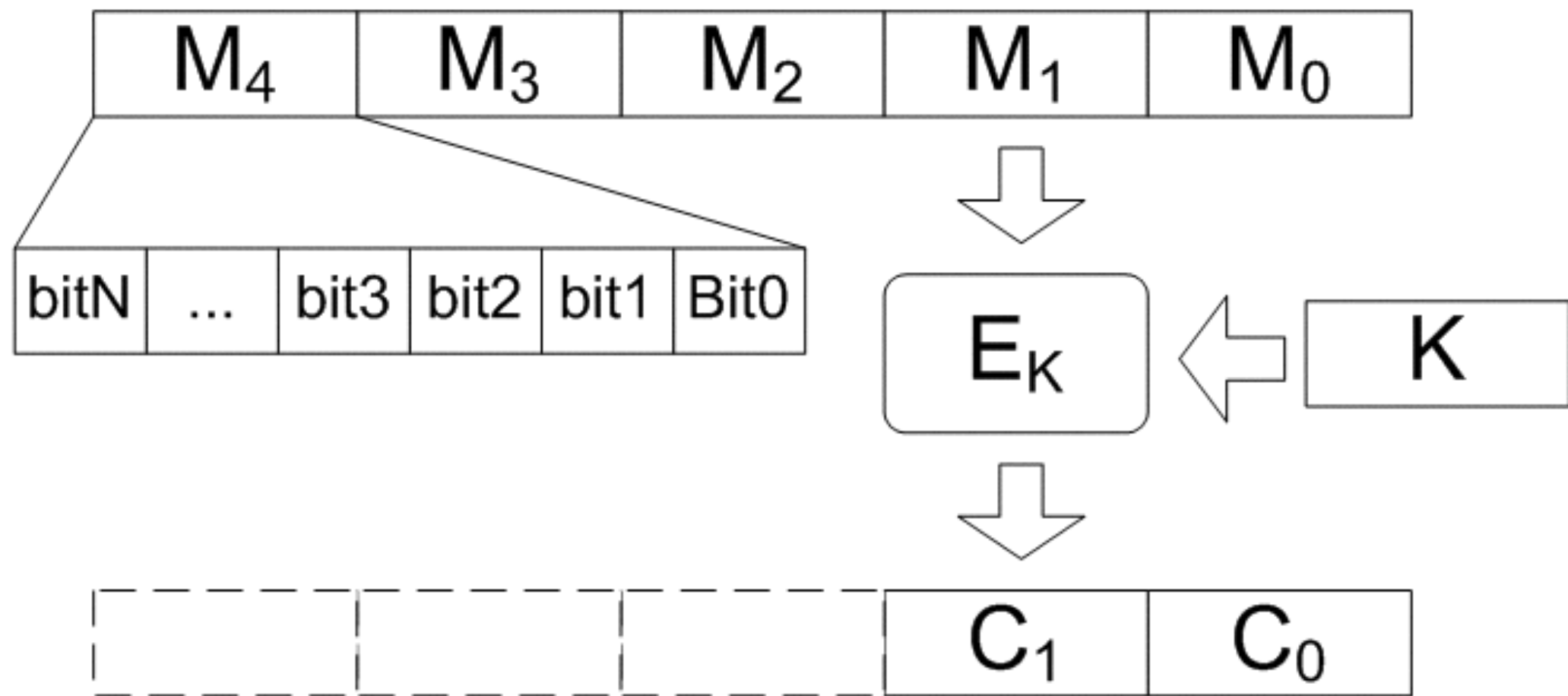


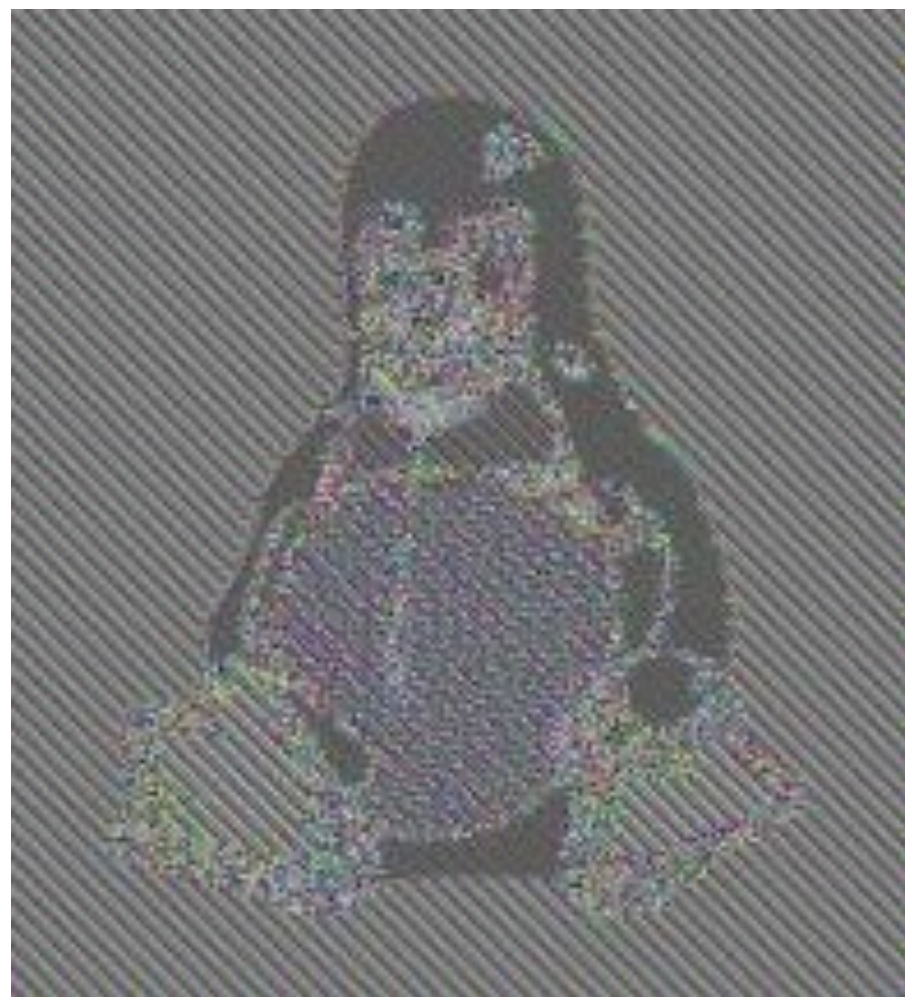


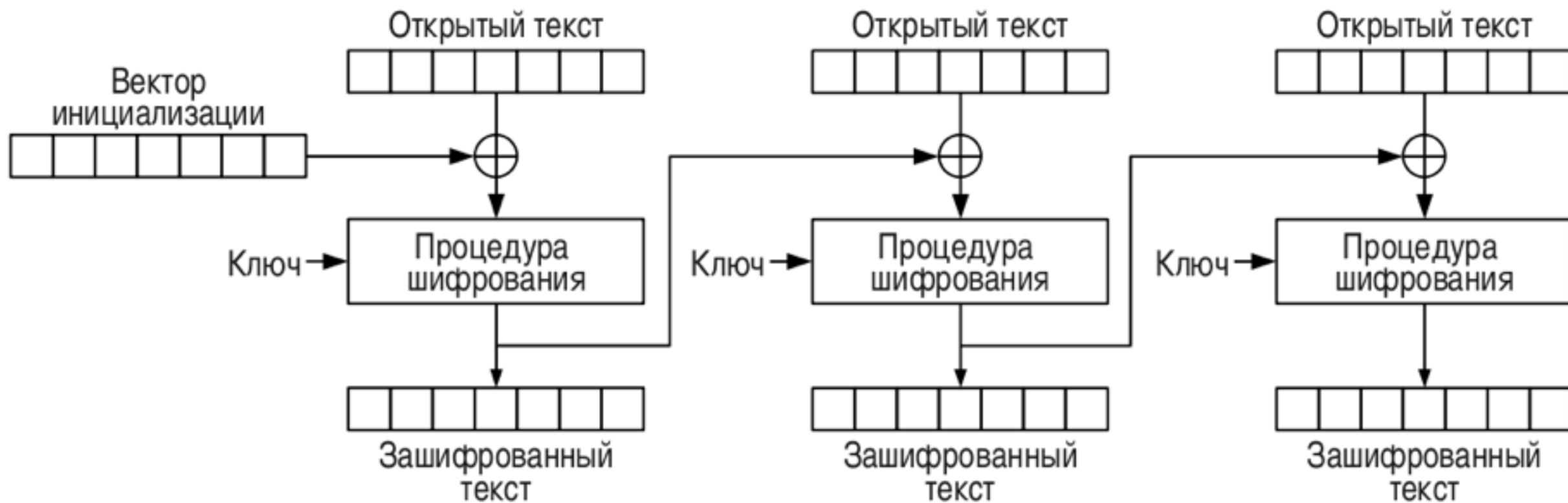




- Типичный блочный шифр: принимает 256-битный вход X , 256-битный ключ K и возвращает 256-битный выход Y
- Как использовать его для шифрования файла размером 1 Мб?



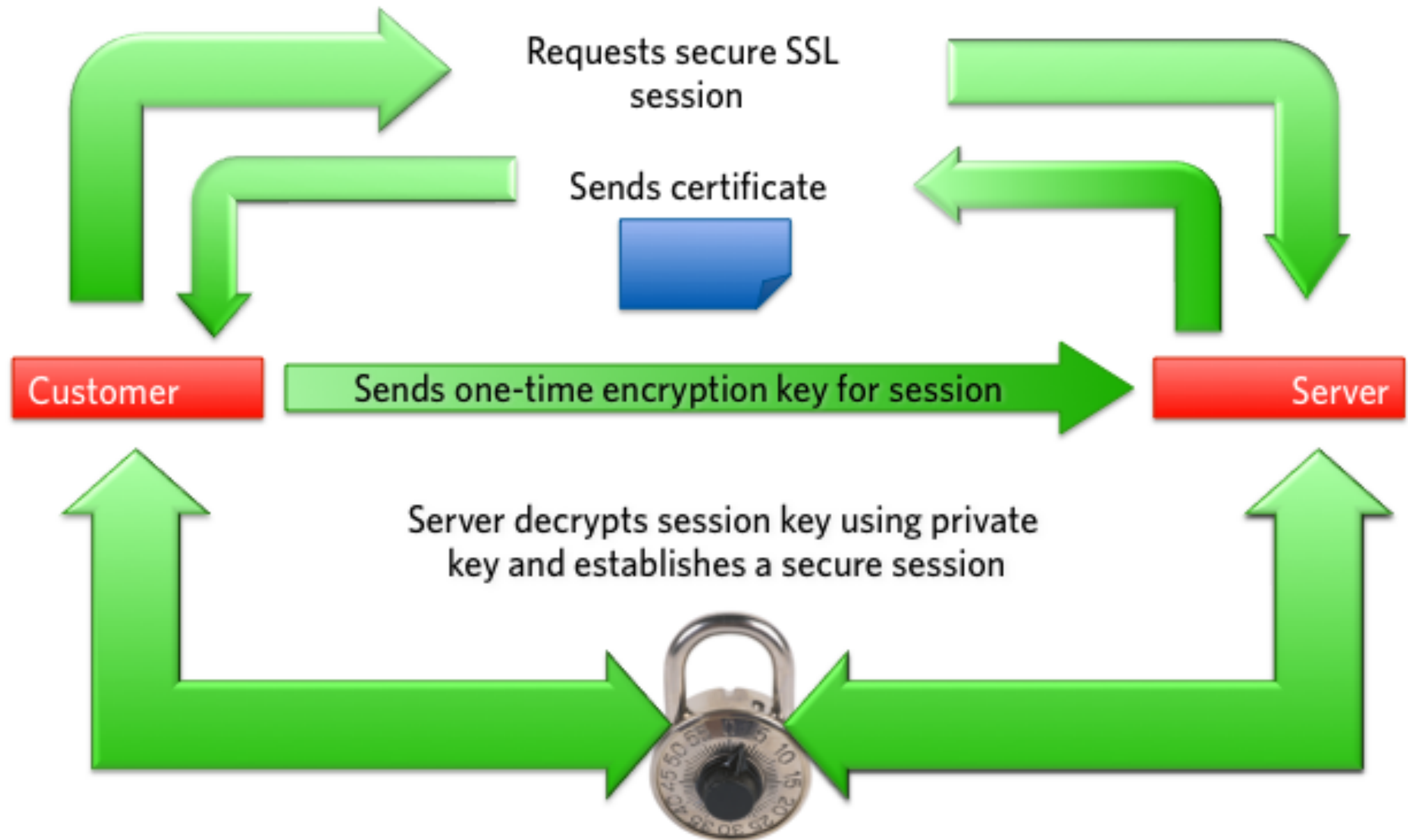




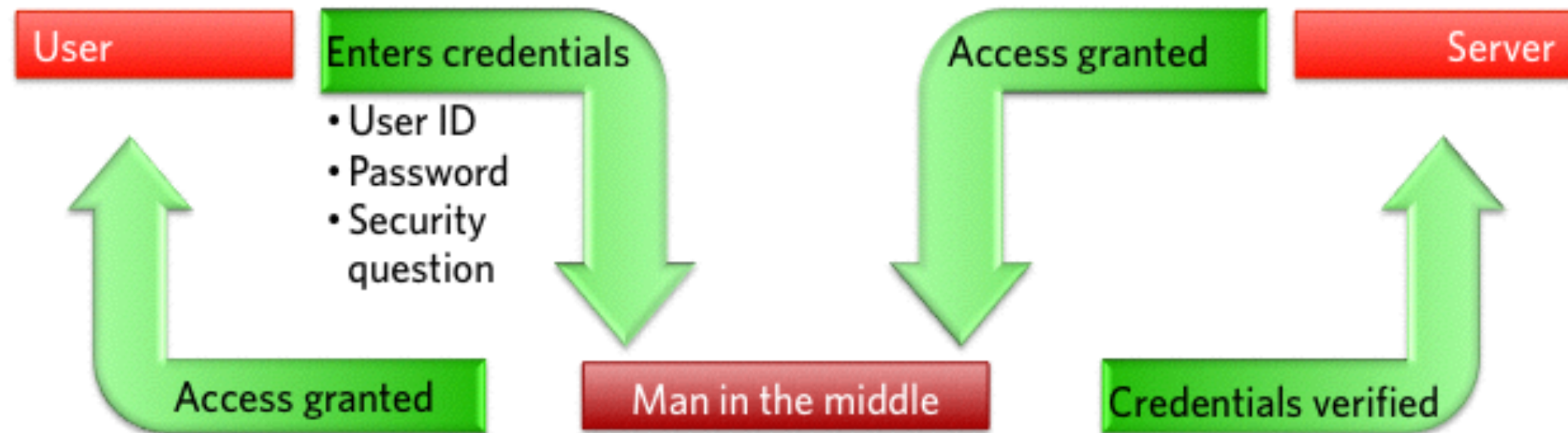


HTTPS

How SSL works



Man in the middle (MITM) attack



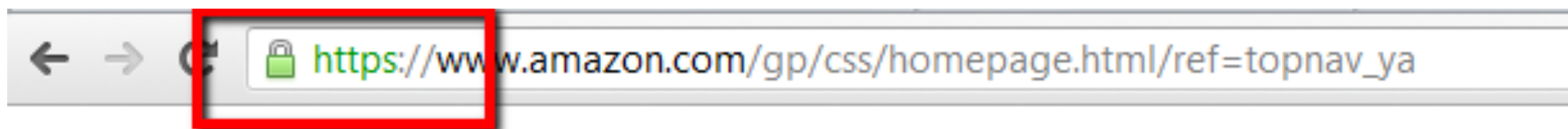


This is probably not the site you are looking for!

You attempted to reach [redacted] but instead you actually reached a server identifying itself as [redacted]. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of [redacted].

You should not proceed, **especially** if you have never seen this warning before for this site.

► [Help me understand](#)



amazon
Join Prime

[Your Amazon.com](#) | [Today's Deals](#) | [Gift Cards](#) | [Sell](#) | [Help](#)

Shop by
Department ▼

Search

Your Account

Orders

[View & Modify Recent Orders](#)

[View, Modify, Track or Cancel an](#)

[Your Orders](#)

Certificate



General

Details

Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

* Refer to the certification authority's statement for details.

Issued to: www.amazon.com

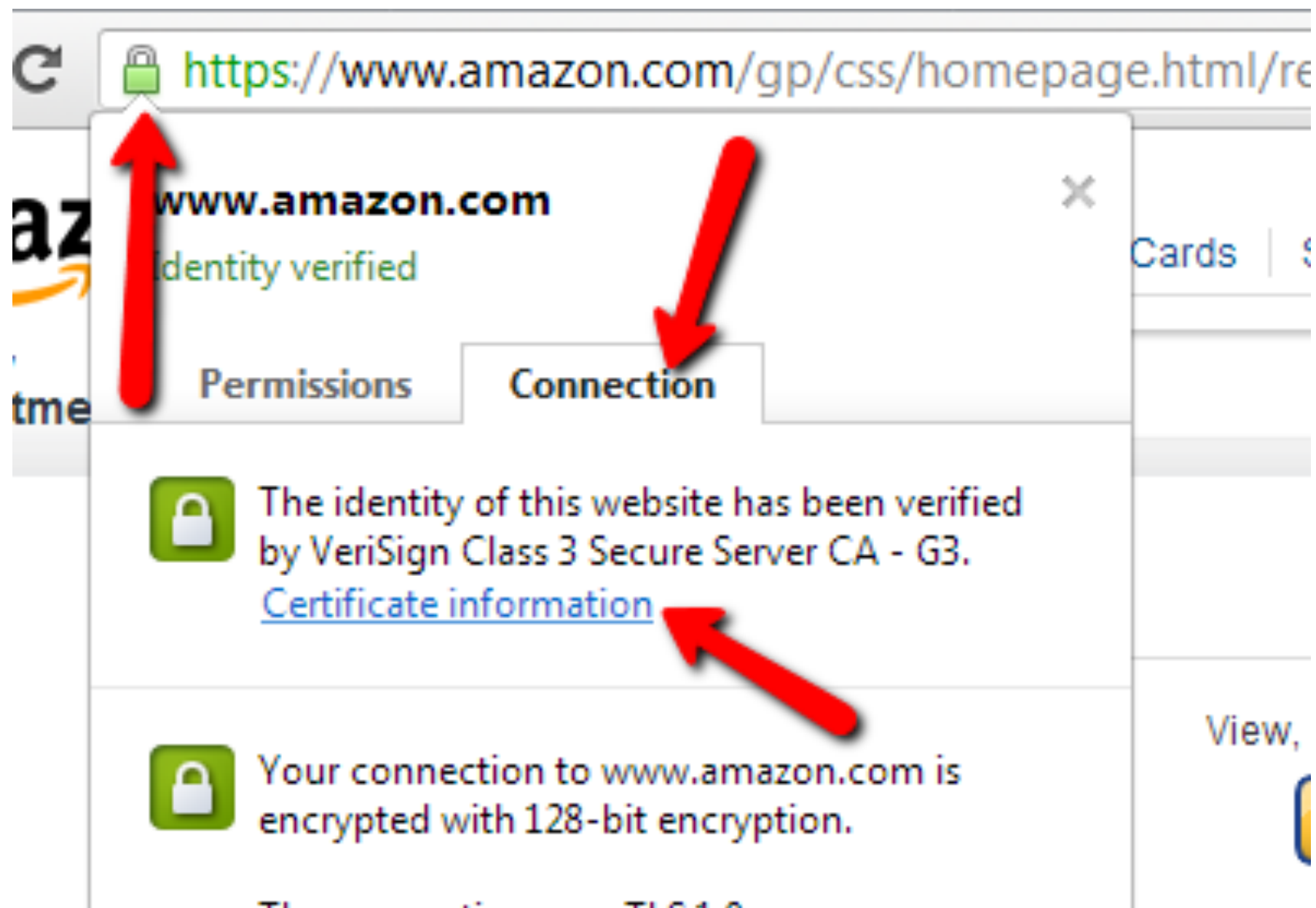
Issued by: VeriSign Class 3 Secure Server CA - G3

Valid from 16/ 05/ 2013 **to** 18/ 05/ 2014

Issuer Statement

Learn more about [certificates](#)

OK



Chain of trust

