



# ВЪВЕДЕНИЕ В КРИПТОГРАФИЯТА

Владислав Драмалиев  
Директор, Фондация „Битхоуп“  
Мениджър маркетинг и общество, æternity



# Contents

1. За мен
2. Какво е криптография?
3. Кратка история на криптографията
  - I. Шифърът на Цезар
  - II. Полиазбучна криптография
  - III. Полиазбучна криптография + случайност
  - IV. Немската машина Енигма
4. Модерна криптография
  - I. Diffie-Hellman
  - II. Симетрична криптография - AES
  - III. Асиметрична криптография – „Публичен ключ“
    - I. Дигитални подписи
    - II. Хеш функции
    - III. Дървета на Меркъл
    - IV. Доказателство за свършена работа



Основател	Съосновател
<ul style="list-style-type: none"><li>• <b>CoinFixer.com</b>   2014</li><li>• <b>BitHope.org</b>   2015</li><li>• <b>CryptoCrowd.org</b>   2017</li></ul>	<ul style="list-style-type: none"><li>• <b>bitcoini.com</b>   2013</li><li>• <b>Bulgarian Bitcoin Association</b>   2014</li><li>• <b>Sofia Crypto Meetup</b>   2016</li></ul>

- В сферата от 2013 г.
- Фокус върху **Sofia Crypto Meetup** и **BitHope.org**
- Част от **æternity blockchain** екипа

# Какво е криптография?

- Наука за криптиране и декриптиране на информация
- От Гръцки – „Kryptos” – таен И “graphia” – текст
- Криптографията е метод на съхранение и прехвърляне на информация
- Основната цел: Само предопределени страни трябва да имат достъп до информацията





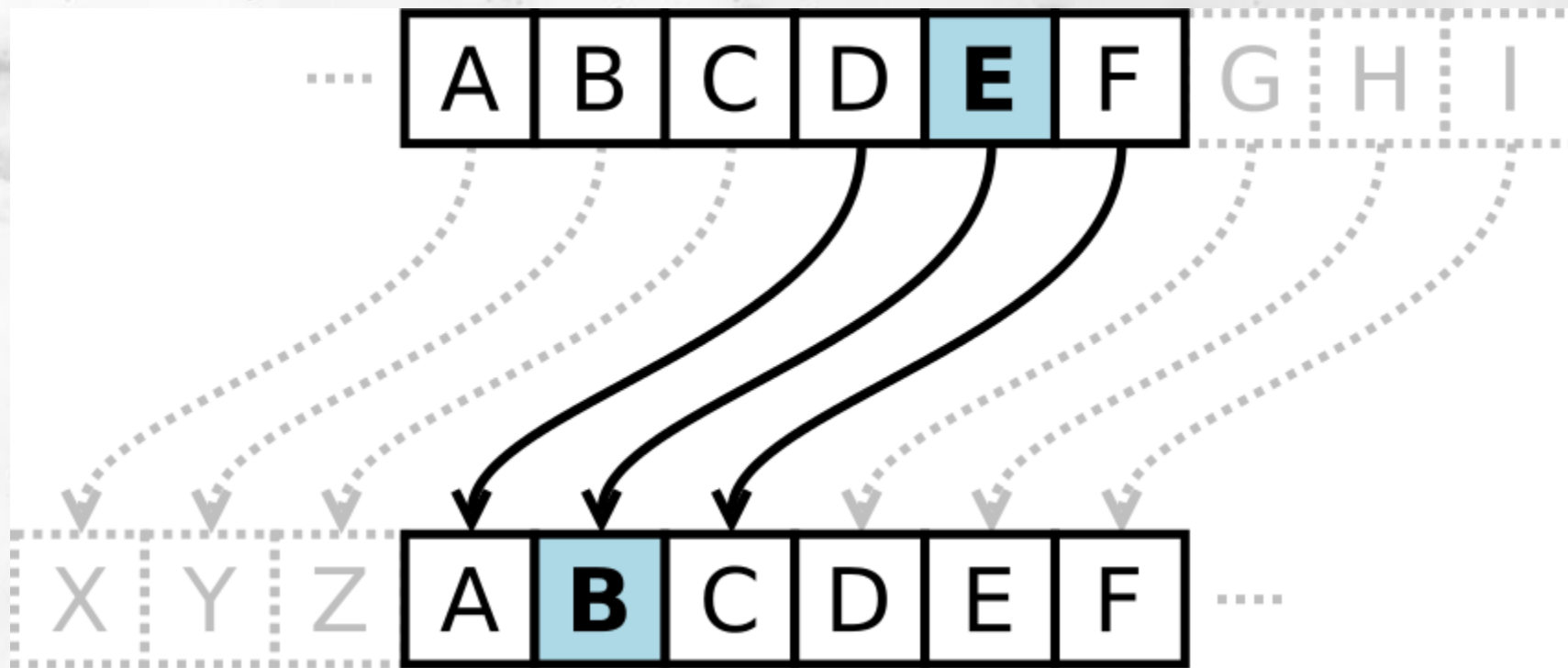
# Кратка история на криптографията

- Хиляди години преди Христа



# Кратка история на криптографията

- Първият по известен пример – Шифърът на Цезар





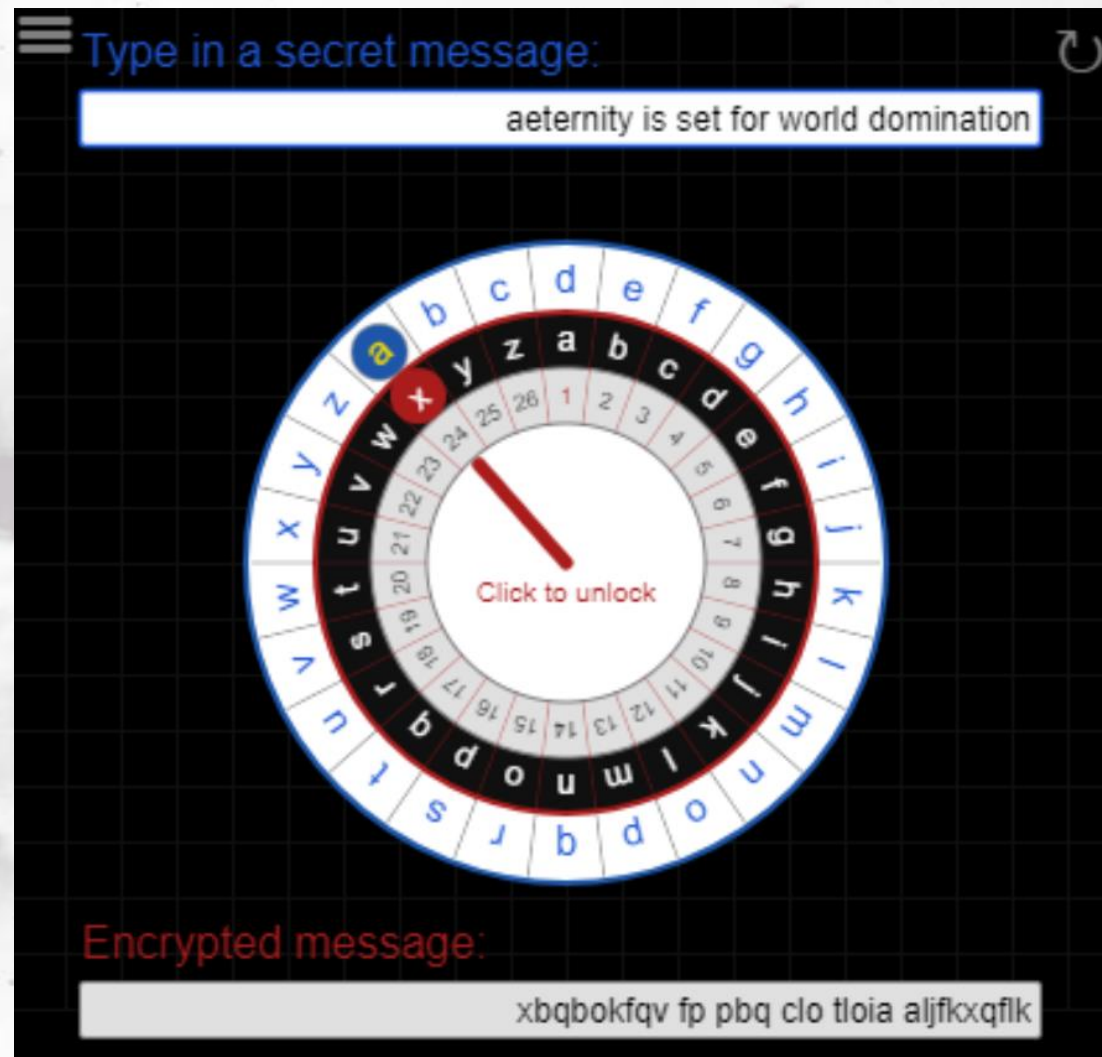
# Кратка история на криптографията

- Първият по известен пример – Шифърът на Цезар

Plain:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Cipher:	XYZABCDEFGHIJKLMNOPQRSTUVWXYZ



# Кратка история на криптографията





# Кратка история на криптографията

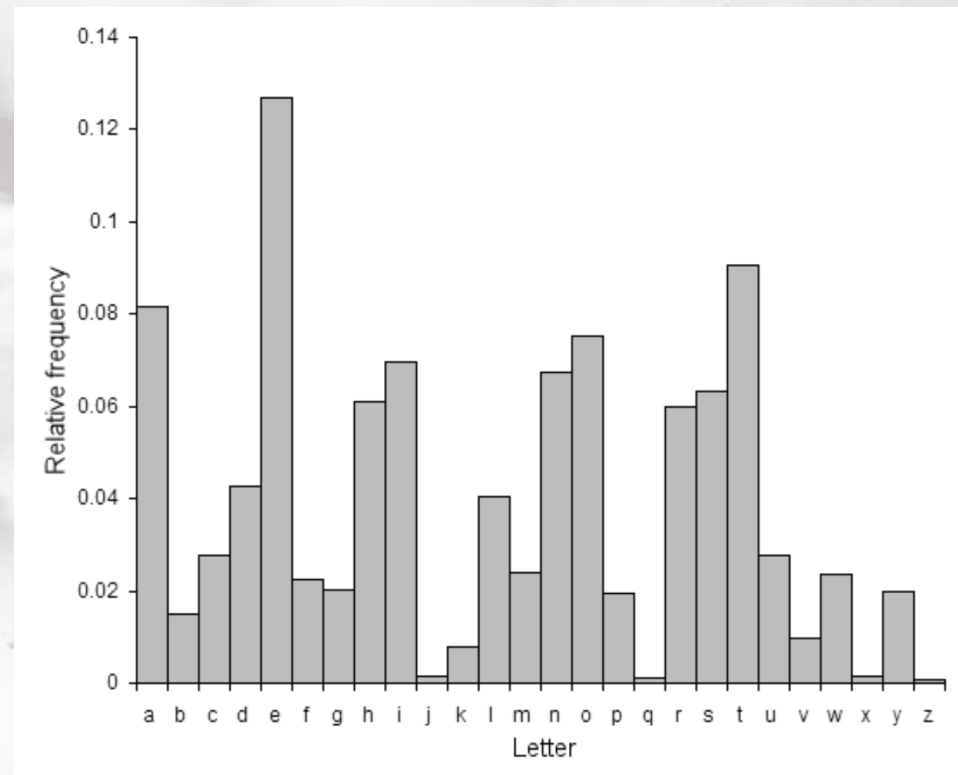
- Очевидно – доста лесен за разшифроване
- Две ситуации:
  1. Знае се, че някаква техника за „замяна“ е била използвана
  2. Знае се, че се използва Шифър на Цезар, но не се знае каква е замяната



# Кратка история на криптографията

При първата ситуация:

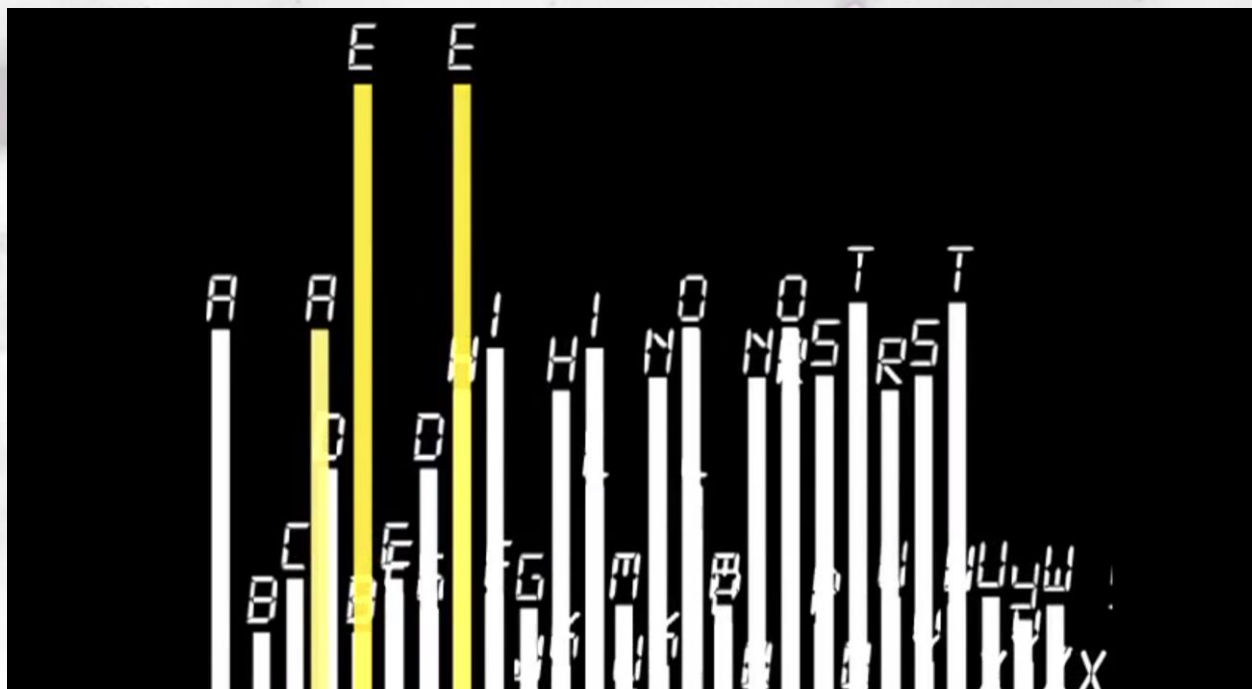
- Необходимо е да се използва „анализ на честотата“



# Кратка история на криптографията

При първата ситуация:

- „Отпечатък“ на езика





# Кратка история на криптографията

При втората ситуация:

- Brute Force атака

Decryption shift	Candidate plaintext
0	exxegoexsrgi
1	dwwdfndwrqfh
2	cvvcemcvqpeg
3	buubdlbupodf
4	attackatonce
5	zsszbjzsnmbd
6	yrryaiyrmlac
...	
23	haahjrhavujl
24	gzzgiqgzutik
25	fyyfhpfytshj



# Кратка история на криптографията

## Полиазбучен подход

- Използва се дума, с която се шифрира съгласно позицията на буквите в азбуката:

**SNAKE -> 19 13 1 11 5**



# Кратка история на криптографията

## Полиазбучен подход

- Използва се дума, с която се шифрира съгласно позицията на буквите в азбуката:

MEET ME AT ELEPHANT LAKE  
13 5 5 20 13 5 1 20 5 12 5 16 8 1 20 12 1 11 5





# Кратка история на криптографията

Полиазбучен подход

MEET ME AT ELEPHANT LAKE

+ +

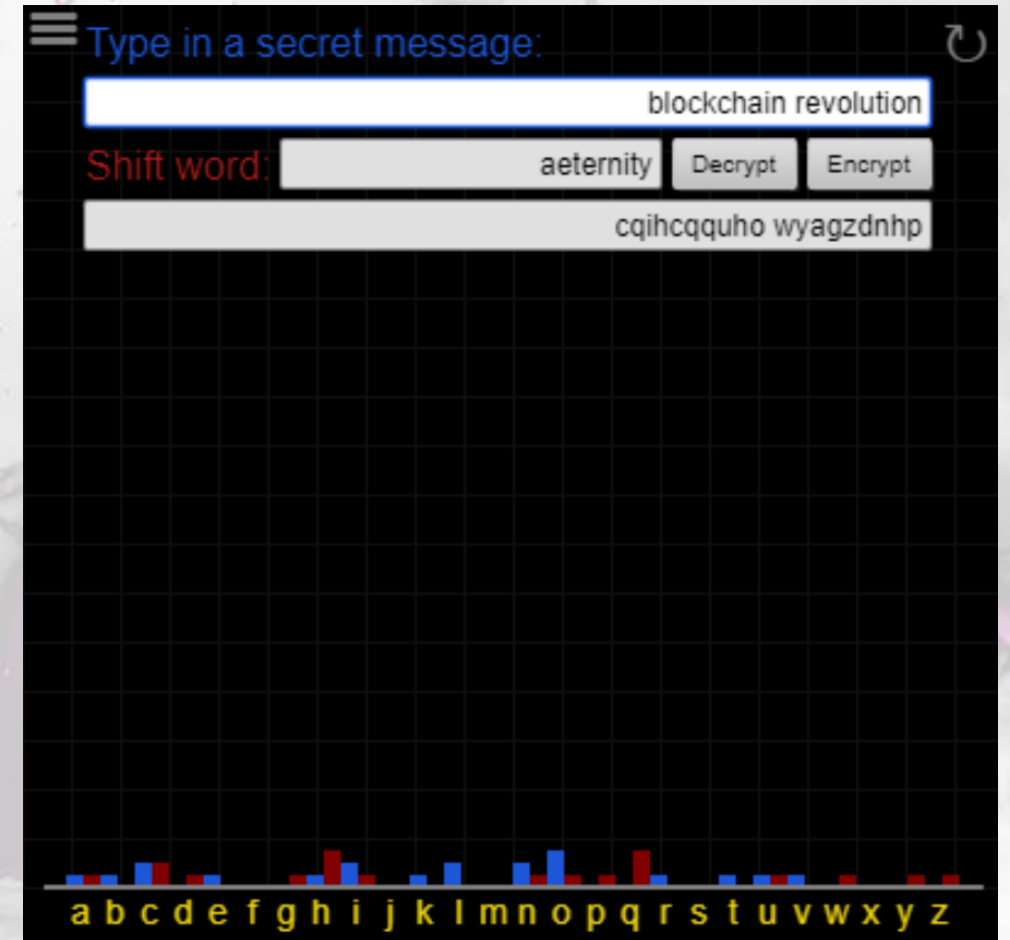
19 13 1 11 5 19 13 1 11 5 19 13 1 11 5 19 13 1 11 5

FSFE RX OU PQXDILSM ZBVV

# Кратка история на криптографията

Полишифърен подход - Как се „разбива“?

- Необходимо е да се идентифицира дължината на шифриращата дума
- Дължина 5 = 5 различни Цезар Шифъра
- Колкото е по-дълга шифриращата дума, толкова по-труден за разшифриране е текстът



# Кратка история на криптографията

Как може да се подобри криптирането на информация?

- Въвеждане на „СЛУЧАЕНОСТ?“





# Кратка история на криптографията

Как може да се подобри криптирането на информация?

- Експлозия на възможните комбинации!

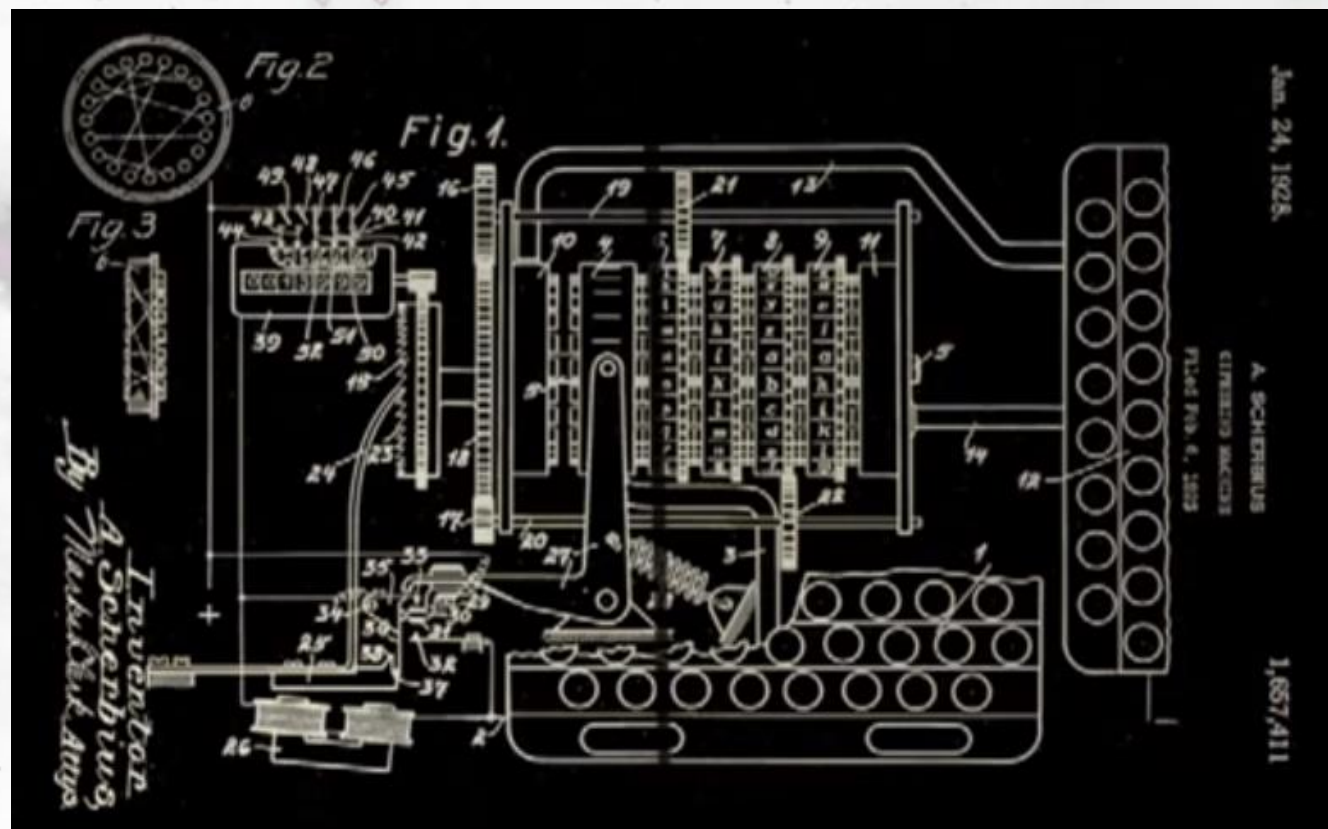
FZXJS  $\rightarrow 26 * 26 * 26 * 26 * 26$

12 000 000 комбинации



# Кратка история на криптографията

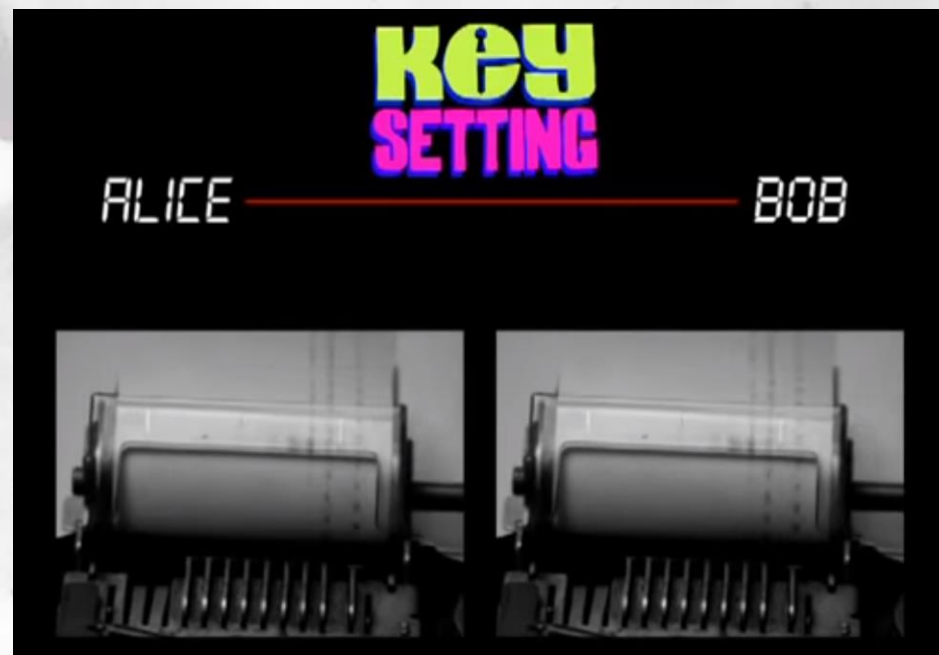
Немската машина за криптиране „Енигма“



# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- Автоматизация на криптирането

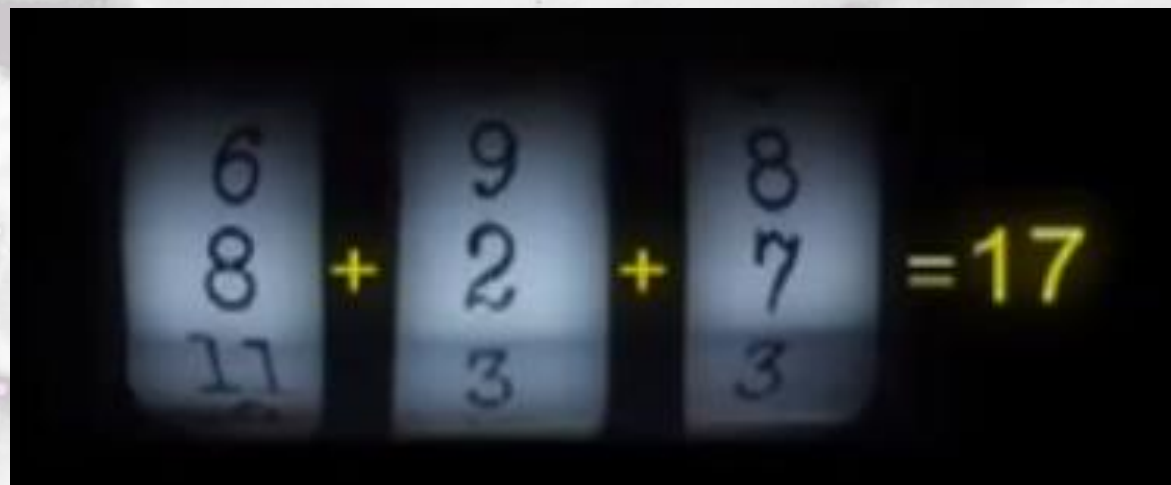




# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- Промяна на „шифъра“ за всяка следваща буква



# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- 3 ротора с по 26 букви, без последователност  $\rightarrow 26 \cdot 26 \cdot 26 = 17\,675$

**17 675 комбинации**



# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- Ако роторите могат да сменят местата си -> 6 комбинации \* 17 675

**106 050 комбинации**



# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- С цел подобряване на сигурността:
  - 4 ротора
  - 60 възможни ротора
- Огромно увеличение на комбинациите!
- Огромен “Key Space”

150 милиона, милиона, милиона комбинации

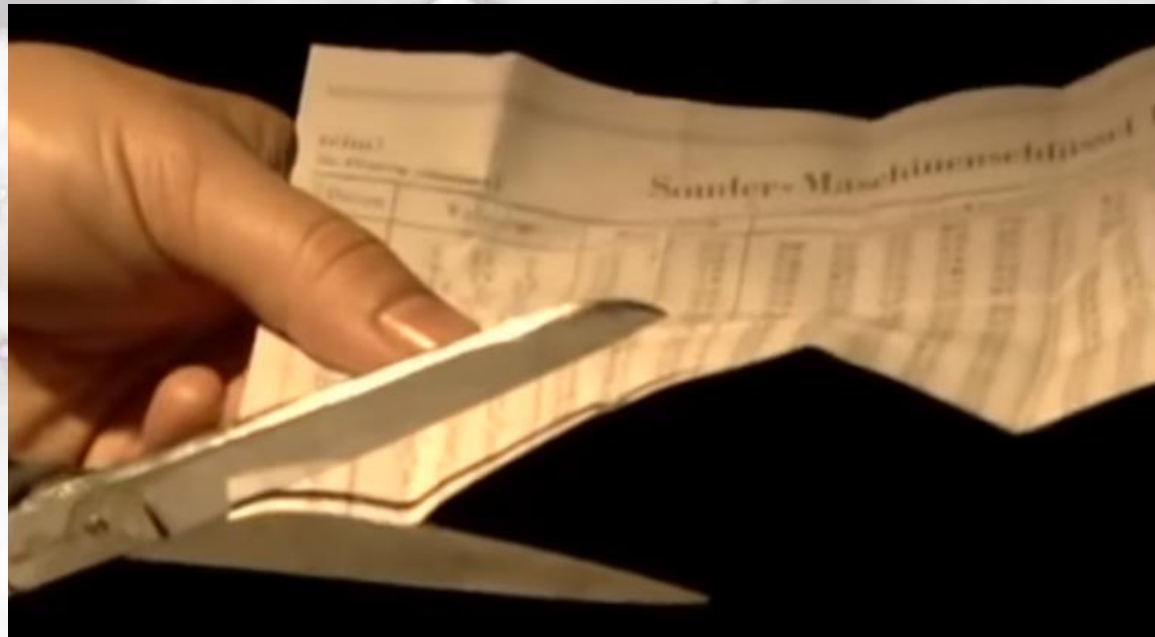




# Кратка история на криптографията

Немската машина за криптиране „Енигма“

- Как са знаели как да използват машината?
- Кои ротори и в какъв ред?



# Кратка история на криптографията

## Немската машина за криптиране „Енигма“

- Два основни проблема
  - Операторът трябва „произволно“ да избере начална позиция
  - Проблем в дизайна – определена буква не може да води до себе си (input/output)

### **Ако:**

- Операторите са хвърляли зарове, за да определят началната позиция
- Определена буква да може да води до себе си



# Кратка история на криптографията

## Основни заключения:

- Теоретичният брой на комбинациите (**key space**) има огромно значение
- Всяка криптирана информация има „отпечатък“ (**fingerprint**)
- Използването на „произволност“ (**entropy**) има огромно значение



# Модерна криптография

- След края на Втората Световна война – Студената война
- Ядрени атаки от междуконтинентални ракети
- 1958 – САЩ и Канада -> NORAD
- 100 автоматизирани радара
- Изпращат информация чрез телефонната мрежа и радио вълни
- Machine-to-machine комуникация – по-бързо вземане на решения
- “Да си онлайн”
- Появяват се компютърните мрежи





# Модерна криптография

## Модерни приложения

- Парични трансфери
- Телекомуникации
- ePassports (Идентификация)
- iPod (protected mp3s)
- Kindle (eBooks)



# Модерна криптография

Секретно споделяне на таен ключ?

Geheime Kommandosache! Jede einzelne Tageschlüssel ist geheim. Mittheilen im Flugzeug verboten! Nr. 00190

Luftwaffen-Maschinen-Schlüssel Nr. 649

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

| Monats-<br>tag | Wellenlage |     |     | Ringstellung | Stichverbindungen  |    |    |    |                          |    |    |    |    |    | Kenngruppen |    |    |    |                 |                 |
|----------------|------------|-----|-----|--------------|--------------------|----|----|----|--------------------------|----|----|----|----|----|-------------|----|----|----|-----------------|-----------------|
|                |            |     |     |              | an der Umkehrwalze |    |    |    | am Sicherheits-<br>breit |    |    |    |    |    |             |    |    |    |                 |                 |
|                |            |     |     |              | 1                  | 2  | 3  | 4  | 5                        | 6  | 7  | 8  | 9  | 10 |             |    |    |    |                 |                 |
| 649            | 31         | I   | V   | III          | 14 09 24           |    |    |    | SZ                       | GT | DV | KU | FO | MY | EW          | JN | IX | LQ | wny dgy ekb rzg |                 |
| 649            | 30         | IV  | III | II           | 05 26 02           |    |    |    | IS                       | EV | MX | RW | DT | UZ | JQ          | AO | CH | NY | kti acw zsi wao |                 |
| 649            | 29         | III | II  | I            | 12 24 03           | KM | AX | PZ | GO                       | DJ | AT | CV | IO | ER | QS          | LW | PZ | PH | ioc acn ovw wvd |                 |
| 649            | 28         | II  | III | V            | 06 08 16           | DI | CN | BR | PV                       | CR | PV | AI | DK | OT | MQ          | EU | BX | LP | lrb cid ude rzh |                 |
| 649            | 27         | III | I   | IV           | 11 03 07           | LT | EQ | HS | UW                       | DY | IN | BV | OR | AM | LO          | PP | HT | EX | woj fbh vct uis |                 |
| 649            | 26         | I   | IV  | V            | 17 22 19           |    |    |    | VZ                       | AL | RT | KO | CO | EI | BJ          | DU | FS | HP | xle gbo uev rxm |                 |
| 649            | 25         | IV  | III | I            | 08 25 12           |    |    |    | OR                       | PV | AD | IT | PK | HJ | LZ          | NS | EQ | CW | ouc uhq uew uit |                 |
| 649            | 24         | V   | I   | IV           | 05 18 14           |    |    |    | TY                       | AS | OW | KV | JM | DR | HX          | GL | CZ | NU | kpl rwl vci tlg |                 |
| 649            | 23         | IV  | II  | I            | 24 12 04           |    |    |    | QV                       | FR | AK | EO | DH | CJ | MZ          | SX | GN | LT | ebn rwm udf tlo |                 |
| 649            | 22         | II  | IV  | V            | 01 09 21           | IU | AS | DV | OL                       | FJ | ES | IM | RX | LV | AY          | OU | BG | WZ | jqc acx mwe wve |                 |
| 649            | 21         | I   | V   | II           | 13 05 19           | PT | OX | EZ | CH                       | RU | HL | FY | OS | GZ | DM          | AW | CE | TV | jpw del mwf wvf |                 |
| 649            | 20         | III | IV  | V            | 24 01 10           | MR | KN | BQ | PW                       | DP | MO | QZ | AU | RY | SV          | JL | GX | DE | jqd cef nvo ysh |                 |
| 649            | 19         | V   | III | I            | 17 25 20           |    |    |    | OX                       | PR | PH | WY | DL | CM | AE          | TZ | JS | GI | idf fpx jwg tlg |                 |
| 649            | 18         | IV  | II  | V            | 15 23 26           |    |    |    | EJ                       | OY | IV | AQ | KW | FX | MT          | PS | LU | BD | lsa bw vcj rxn  |                 |
| 649            | 17         | I   | IV  | II           | 21 10 06           |    |    |    | IR                       | KZ | LS | EM | OV | OY | QX          | AP | JP | BU | mae hzi sog ysi |                 |
| 649            | 16         | V   | II  | III          | 08 16 13           |    |    |    | HM                       | JO | DI | NR | BY | XZ | OS          | PU | PQ | CT | tdp dhh fkb uiv |                 |
| 649            | 15         | II  | IV  | I            | 01 03 07           |    |    |    | DS                       | HY | MR | GW | LX | AJ | BQ          | CO | IP | NT | ldw hzj soh wvg |                 |
| 649            | 14         | IV  | I   | V            | 15 11 05           | AI | BT | MV | HU                       | GM | JR | KS | IY | HZ | PL          | AX | BT | CQ | imz noa tjv xtk |                 |
| 649            | 13         | I   | III | II           | 13 20 03           | FW | EL | DG | KN                       | LY | AG | KM | BR | IQ | JU          | HV | SW | ET | CX              | zgr dgz gjo ryg |
| 649            | 12         | V   | I   | IV           | 18 10 07           |    |    |    | MU                       | BP | CY | RZ | KX | AN | JT          | DG | IL | FX | zdy rkf tjw xtl |                 |
| 649            | 11         | II  | IV  | III          | 02 26 15           | RZ | OQ | CP | SX                       | KN | UY | HR | PW | FM | BO          | EZ | QT | DX | JV              | zea rjy soi wvh |
| 649            | 10         | III | V   | IV           | 23 21 01           |    |    |    | LR                       | IK | MS | QU | HW | PT | OO          | VX | PZ | EN | lrc zbx vbm rxo |                 |
| 649            | 9          | V   | I   | III          | 16 04 08           |    |    |    | QY                       | BS | LN | KT | AP | IU | DW          | HO | RV | JZ | edj eyr vby tih |                 |
| 649            | 8          | IV  | II  | V            | 13 19 25           |    |    |    | PI                       | NQ | SY | CU | BZ | AH | EL          | TX | DO | KP | yiz dha eke tli |                 |
| 649            | 7          | I   | IV  | II           | 09 03 22           |    |    |    | UX                       | IZ | HN | BK | OQ | CP | FT          | JY | MW | AR | lan dgb zsj wbi |                 |
| 649            | 6          | III | I   | V            | 11 18 14           |    |    |    | DQ                       | GU | BW | NP | HK | AZ | CI          | PO | JX | VY | lao cft zsk wbj |                 |
| 649            | 5          | V   | II  | IV           | 23 02 25           | IL | AP | EU | HO                       | MV | CL | OK | OQ | BI | PU          | HS | FX | NW | lju cdr iye waj |                 |
| 649            | 4          | II  | IV  | I            | 04 21 09           | QT | WZ | KV | GM                       | AC | BL | OZ | EK | QW | OP          | SU | DH | JM | tsb zby vcy ujb |                 |
| 649            | 3          | V   | I   | III          | 19 11 06           | BF | NR | DX | CS                       | KR | MP | CN | BP | EH | DZ          | IW | AV | GJ | LO              | lap owd iwu wak |
| 649            | 2          | IV  | V   | I            | 16 14 02           |    |    |    | BN                       | HU | EG | PY | KQ | CP | OS          | JW | AI | VZ | aqd bdy iyf xtd |                 |
| 649            | 1          | III | I   | IV           | 23 12 10           |    |    |    | DP                       | BM | NZ | CK | QV | HQ | AP          | UY | SW | JO | kgl cdf gic wuv |                 |



# Модерна криптография

## Откритието на Diffie-Hellman

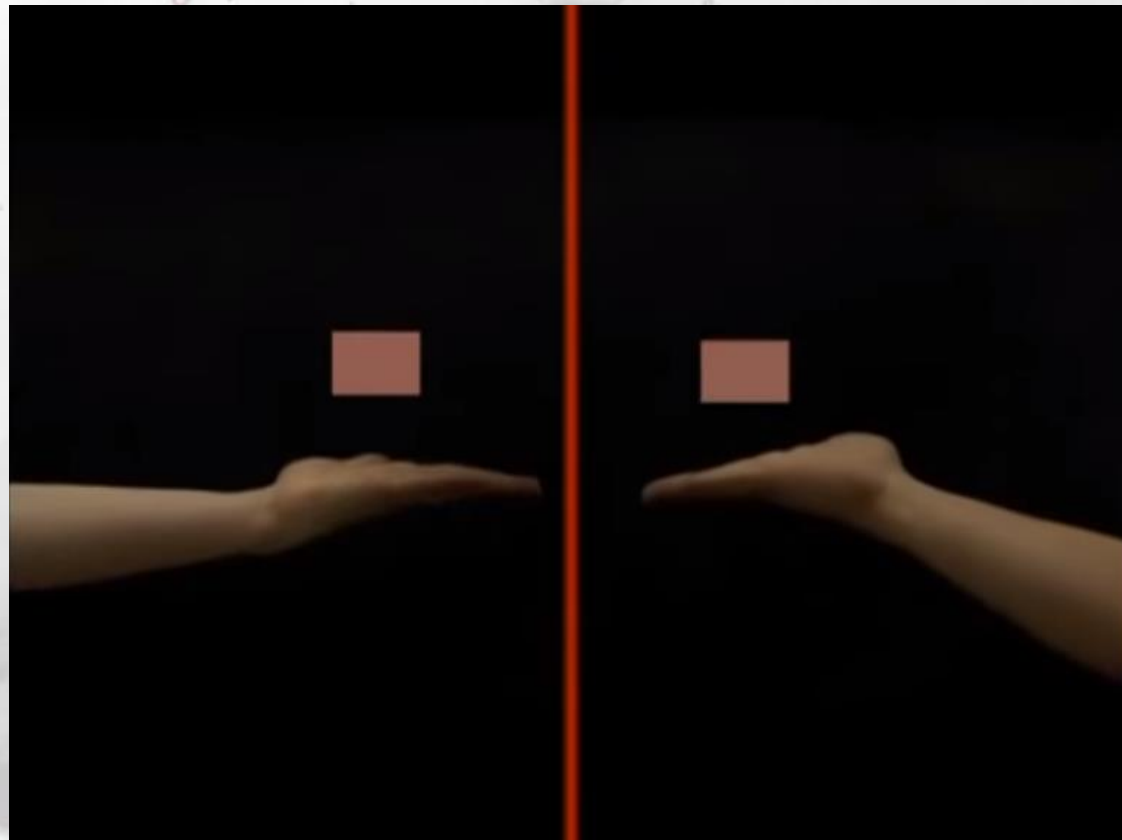
- Как могат две страни да се съгласят относно таен цвят, без той да бъде разбран от трета страна?

Трикът се базира на две неща:

1. Два цвята се смесват лесно
2. Трудно е от микс да се разбере кои цветове са били миксирани

Това е добър „катианар“

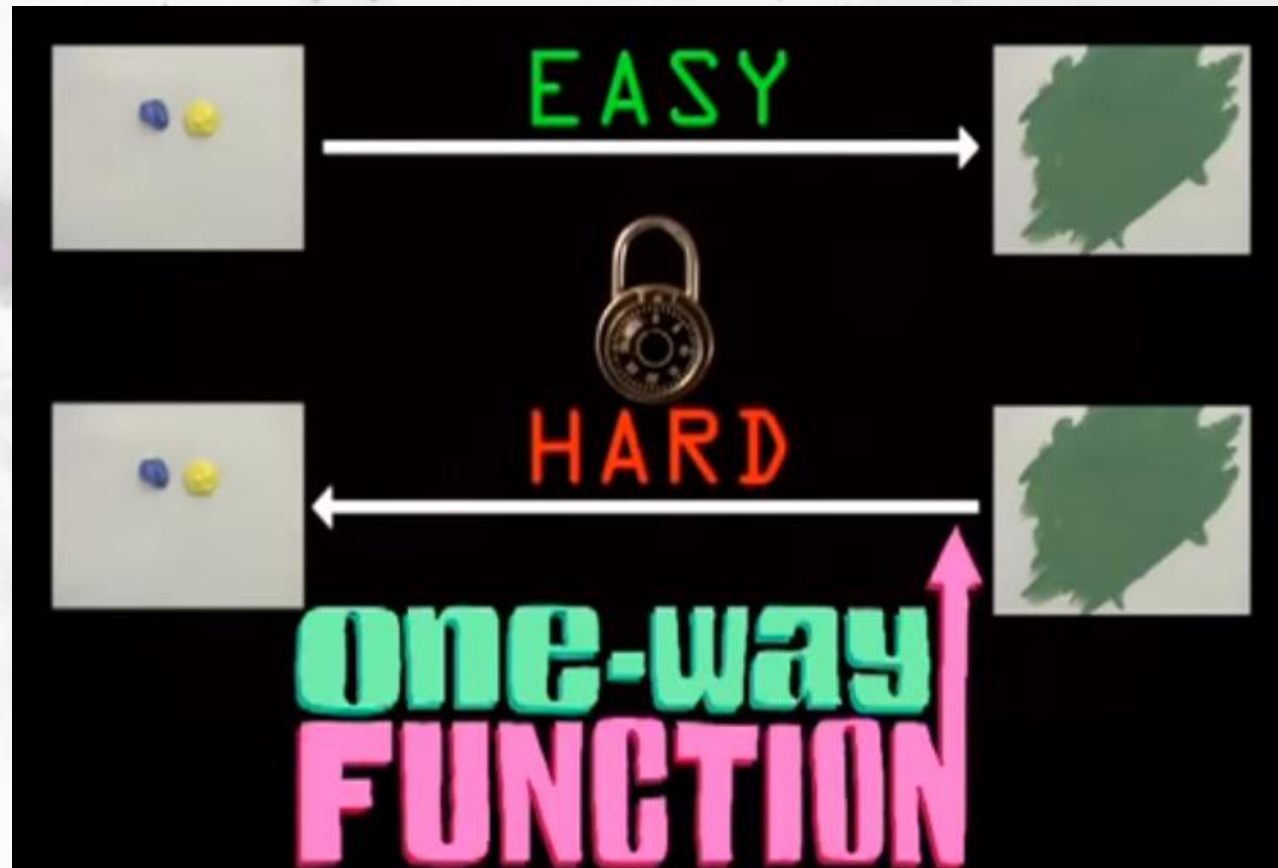
**Лесно в едната посока, труден в другата**



# Модерна криптография

Това е добър „катунар“

Лесно в едната посока, трудно в другата

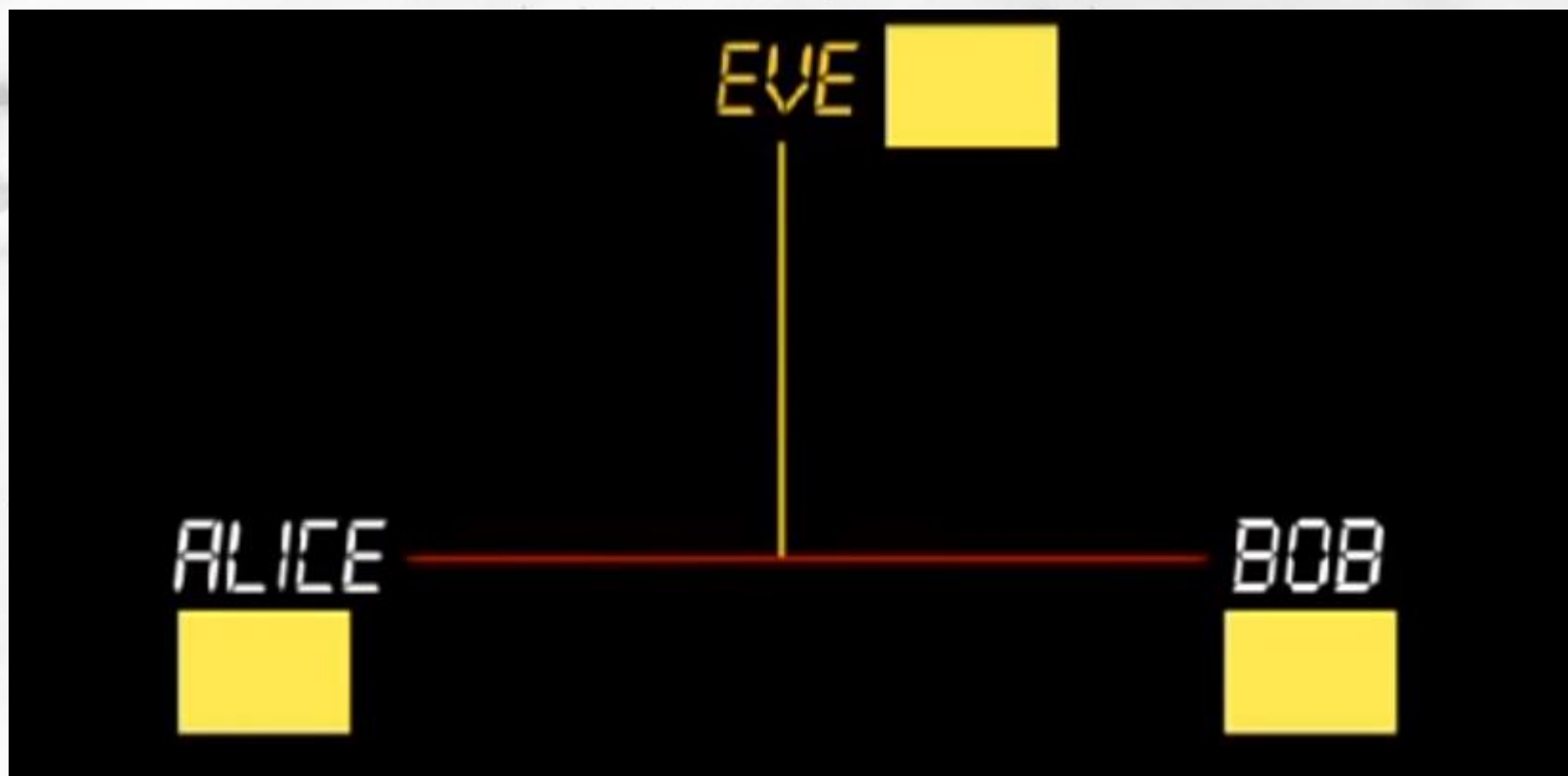




# Модерна криптография

Как работи системата?

**1. Избира се начален цвят**



# Модерна криптография

Как работи системата?

**2. Двете страни си избират произволен цвят (червено и синьо)**

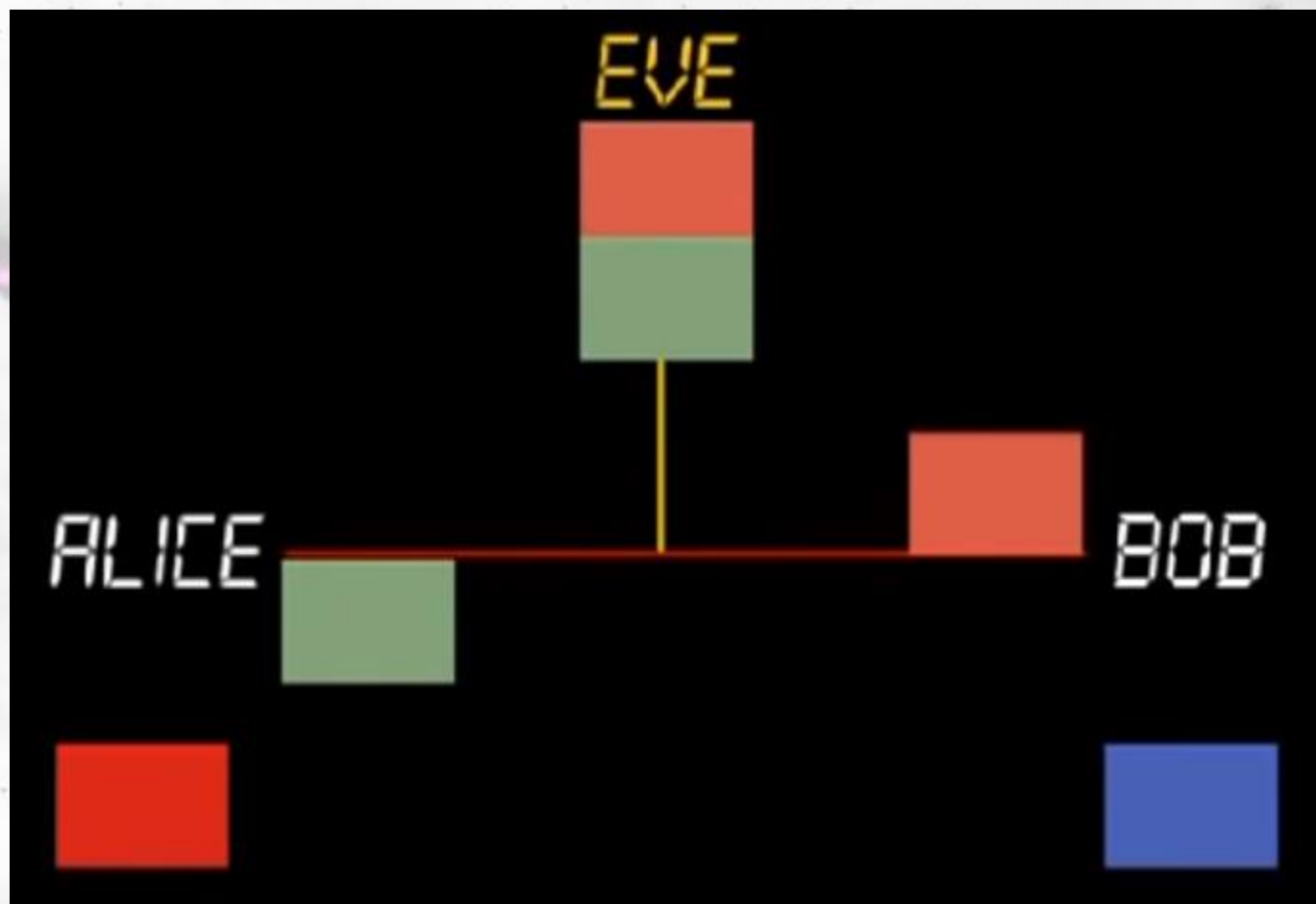
**3. Смесват цветовете**



# Модерна криптография

Как работи системата?

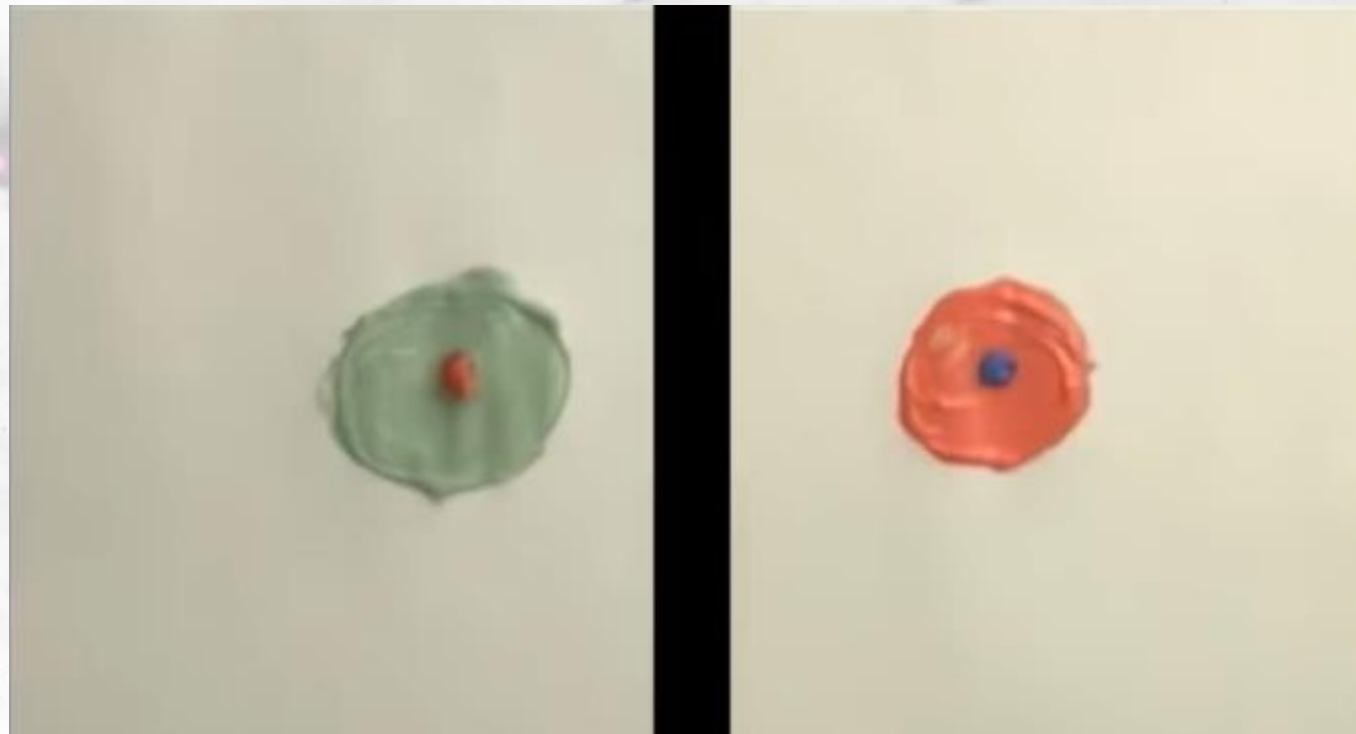
## 4. Смесите се изпращат



# Модерна криптография

Как работи системата?

**5. Двете страни добавят техните цветове към сместа → споделен цвят!**

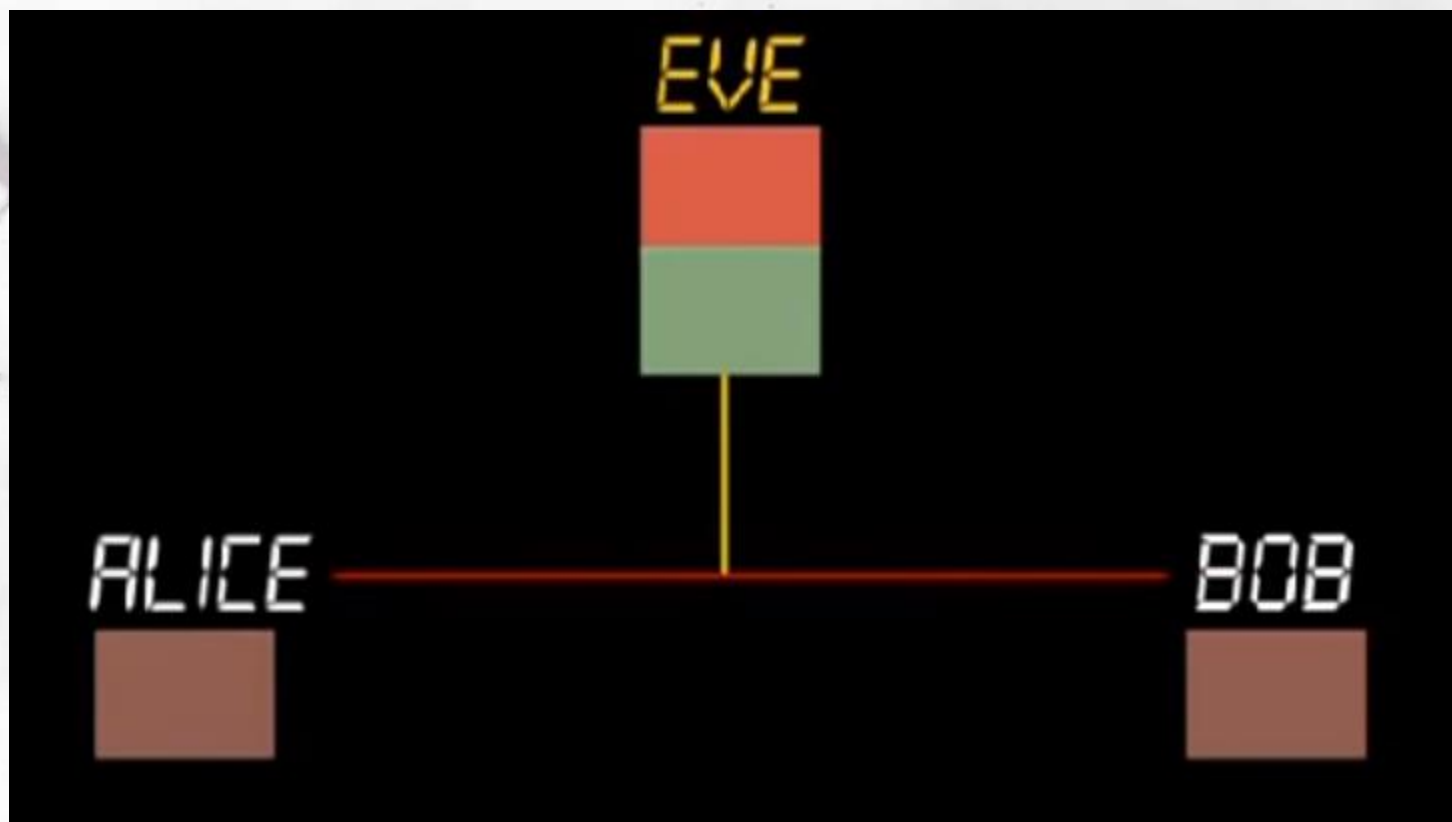




# Модерна криптография

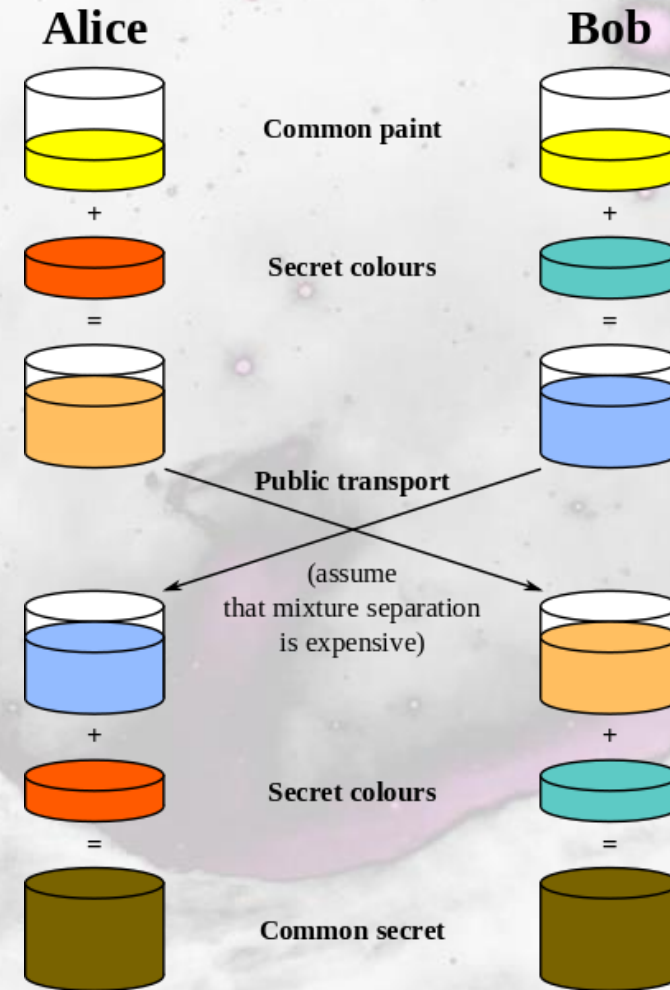
Как работи системата?

**6. Третата страна няма как да разбере кой е цветът – има само смесите**



# Модерна криптография

Как работи системата?

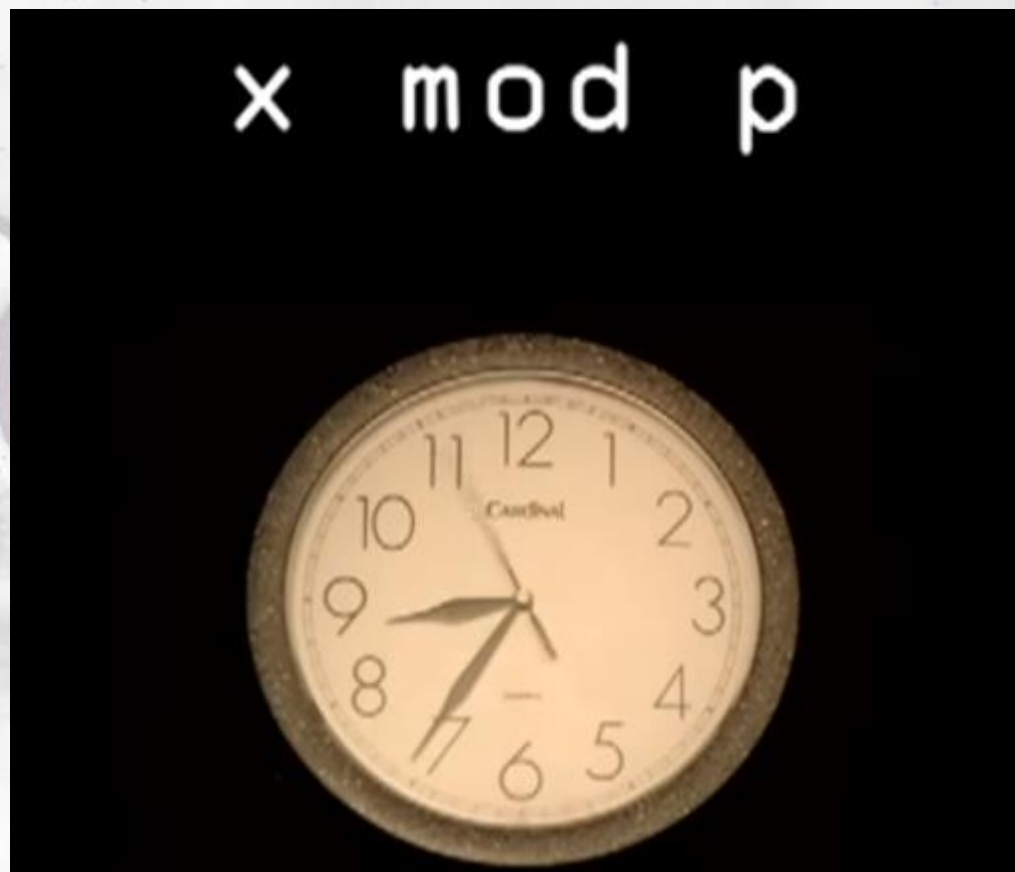


# Модерна криптография

Математически еквивалент

Модулна Аритметика (Часовникова Аритметика)

- $X$  = генератор
- $P$  = прост модул



# Модерна криптография

Математически еквивалент – Модулна Аритметика (Часовникова Аритметика)

$$46 \bmod 12 = 10$$


- Върже с дължина 46, което се увива около часовник





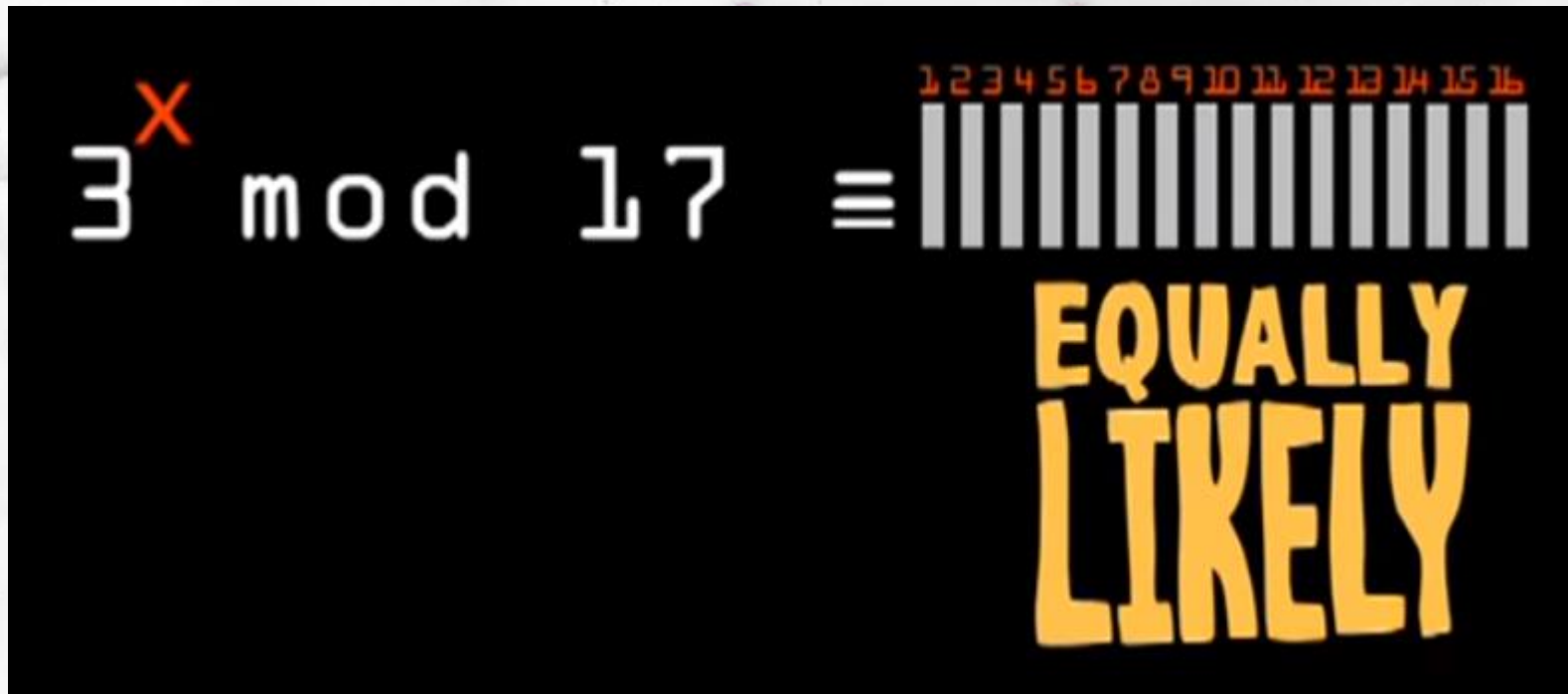
# Модерна криптография

Модулна Аритметика (Часовникова Аритметика)

$$3^{10} \bmod 17 \equiv$$


# Модерна криптография

Модулна Аритметика (Часовникова Аритметика)



# Модерна криптография

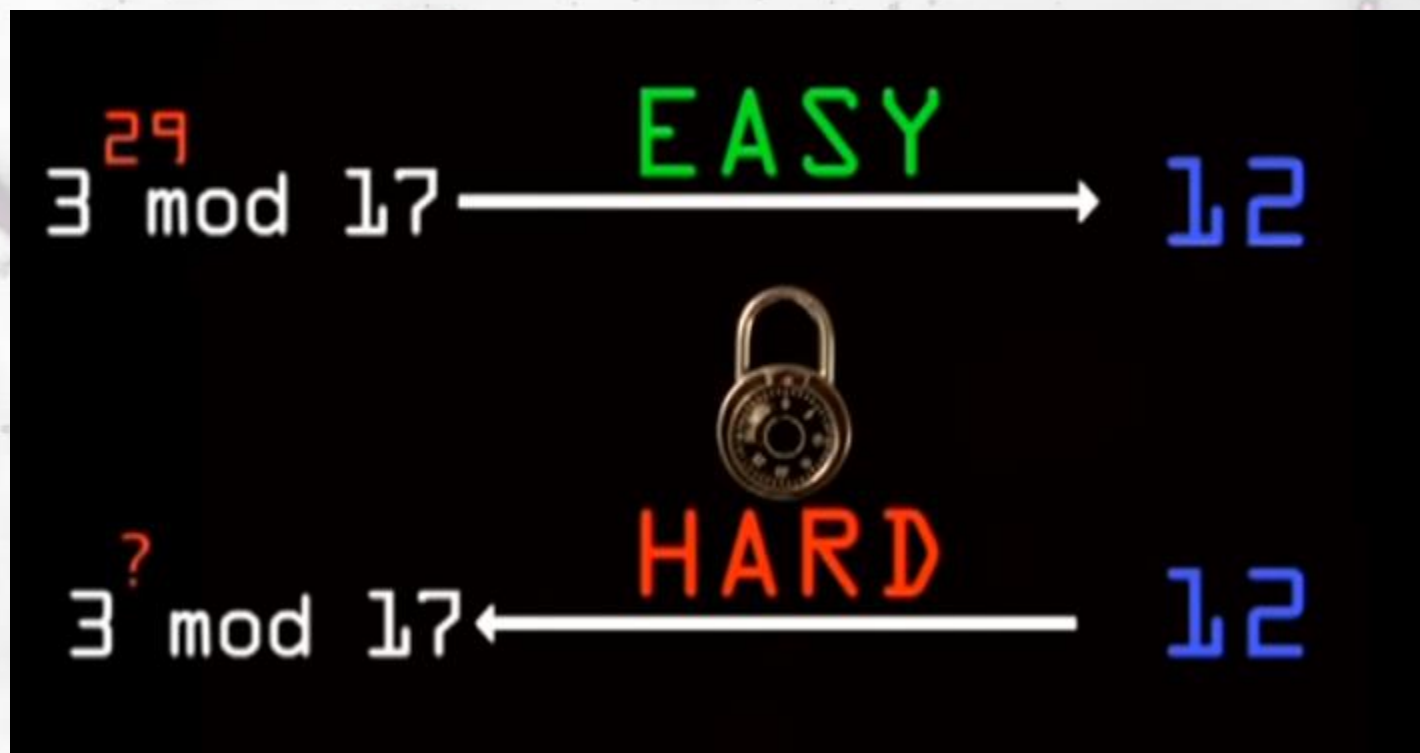
Модулна Аритметика (Часовникова Аритметика)

$$3^? \bmod 17 \equiv 12$$



# Модерна криптография

Модулна Аритметика (Часовникова Аритметика)



Само „проба-грешка“





# Модерна криптография

Модулна Аритметика (Часовникова Аритметика)

Кратко видео



# Модерна криптография

Модулна Аритметика (Часовникова Аритметика)

- С малки числа – „Проба/грешка“ подходът работи
- Ако се използват числа дълги стотици цифри – хиляди години
- Дори с помощта на цялата компютърна мощност на света



# Модерна криптография

## Модулна Аритметика (Часовникова Аритметика)

### Проблеми:

- Един същ ключ се използва за криптиране и декриптиране
- Ключът трябва да се запази таен
  - При съхранение
  - При използване
- Трябва да се случи едновременно (handshake)

**Този начин на криптиране се нарича „симетричен“ (+ по-бърз)**

- AES



Модерна криптография

Симетрична криптография





# Модерна криптография

## AES – симетрична криптография

- Използва се от NSA за топ-секретна информация
- 331,252 компютъра и над 1,757 дни - 64-bit RC5
- AES - 128-bits, 192-bits, and 256-bits
- Ако всеки от 7те милиарда хора на света има 10 компютъра и тества 1 милиард комбинации в секунда ->

**77,000,000,000,000,000,000,000 години (128-bit)!**



# Модерна криптография

## Асиметрично криптиране – „Public Key“ Криптография

- По-подходяща за комуникация
- Използват се два ключа – един за криптиране, един за декриптиране
- Bitcoin! (най-накрая)
- Как работи асиметричното криптиране?



# Модерна криптография

## Асиметрично криптиране (Public Key)

Три елемента:

- Ключ (таен)
- Катионар (публичен)
- Парола (тайна)



# Модерна криптография

## Асиметрично криптиране (Public Key)

### Процес:

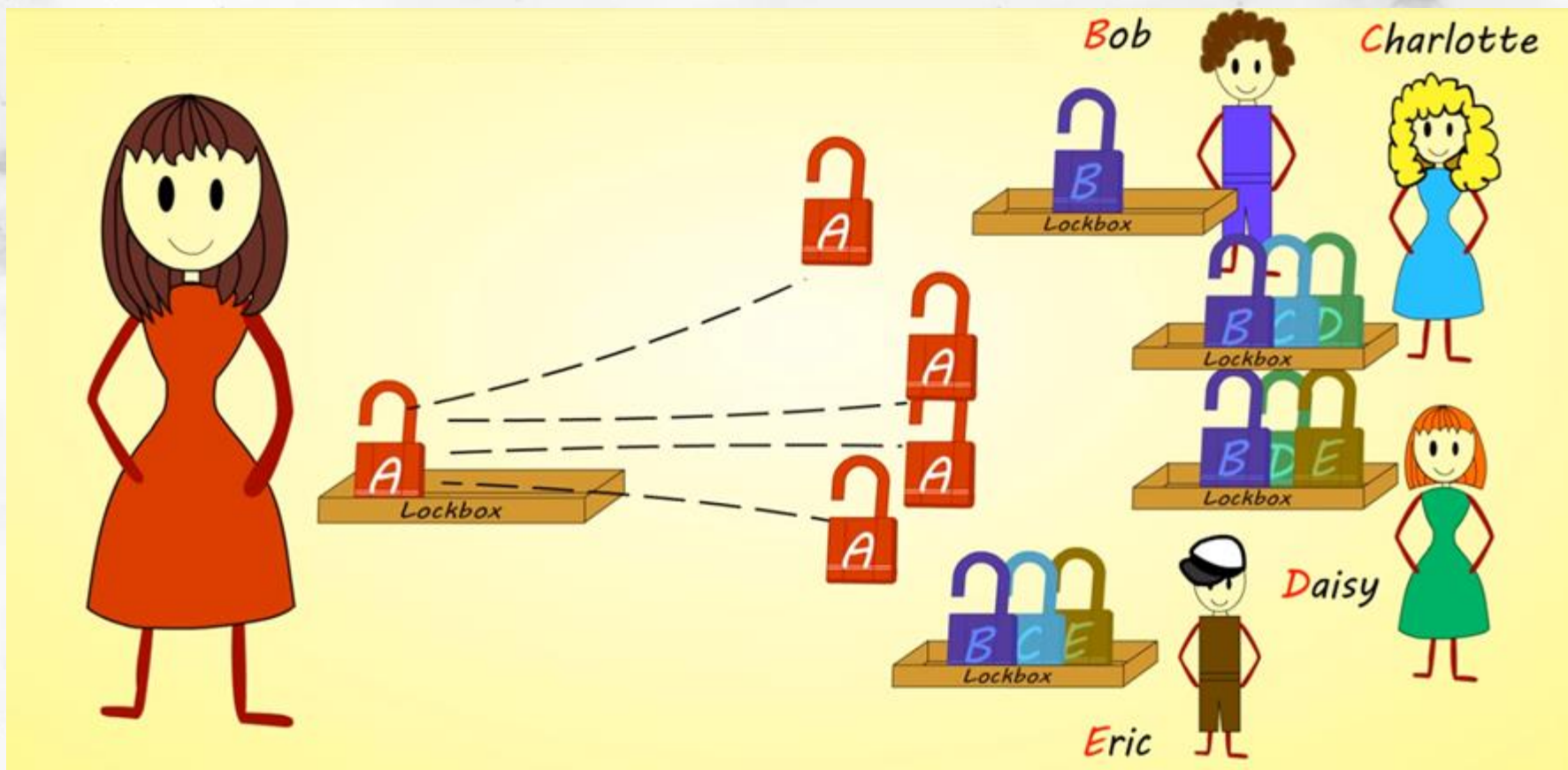
1. Тайният ключ – защитен с паролата
2. Катарът се използва за заключване/криптиране на информация
3. За да може някой да изпраща информация – необходим му е катарът





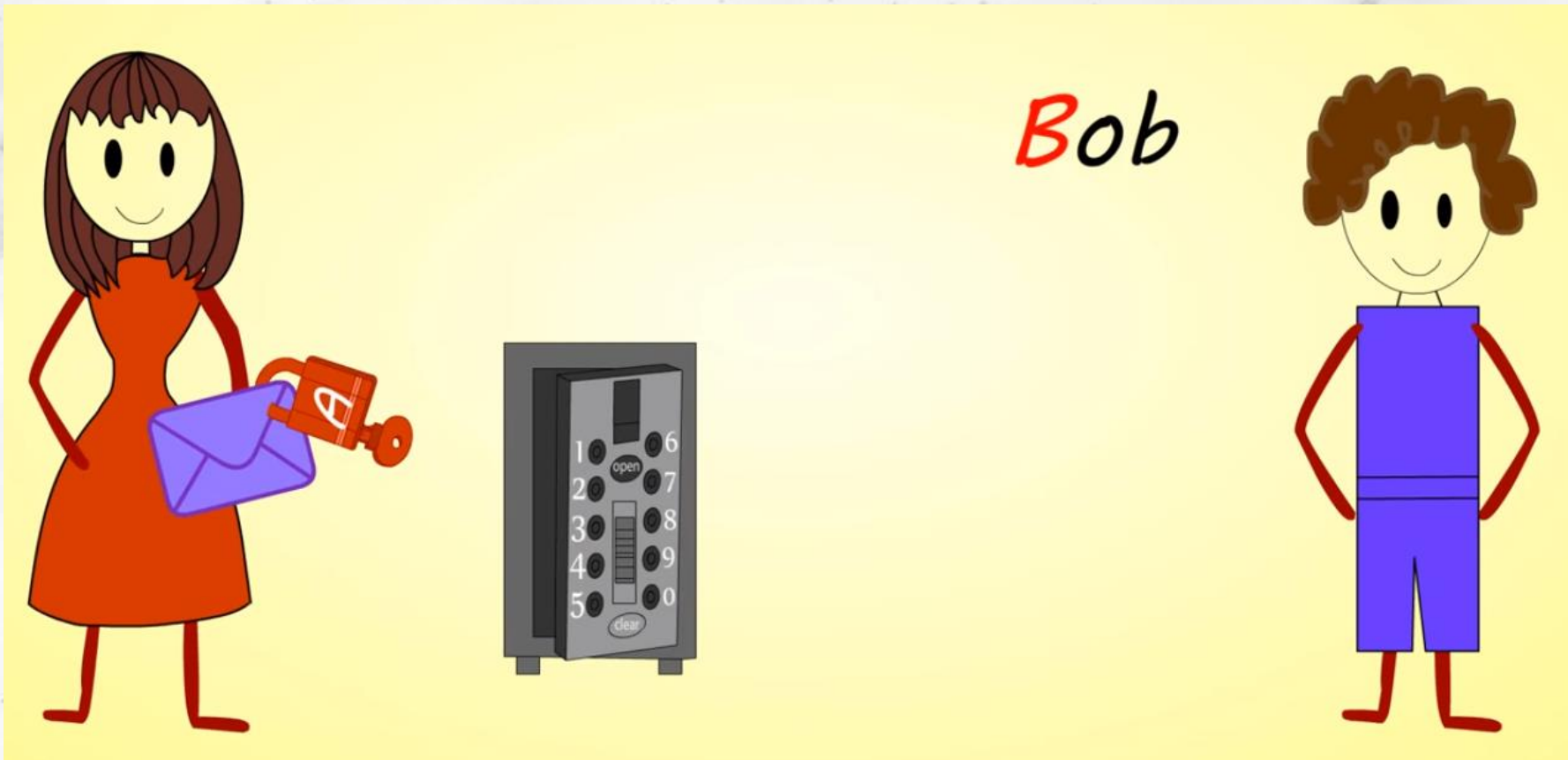
# Модерна криптография

## Асиметрично криптиране (Public Key)



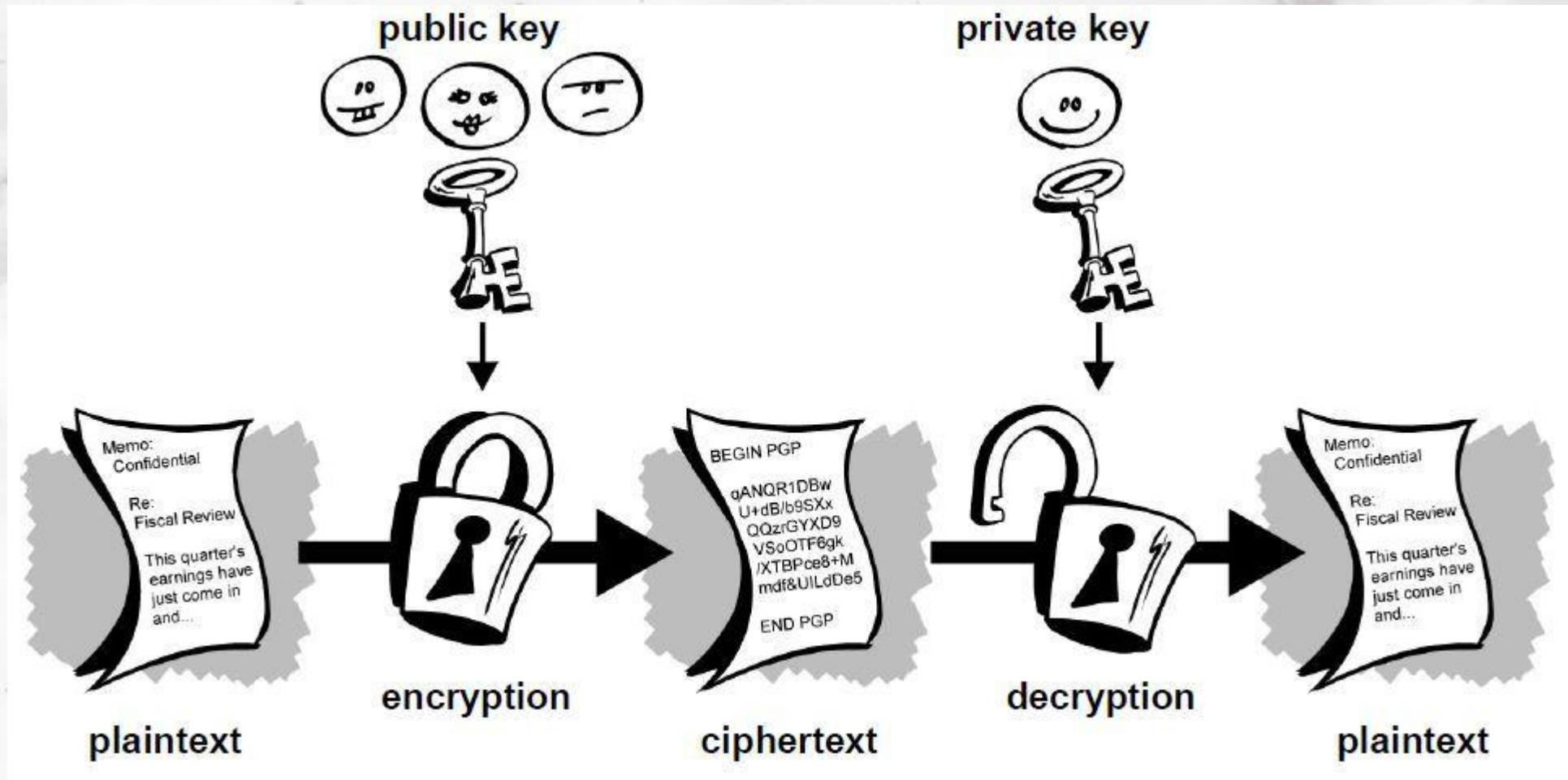
# Модерна криптография

## Асиметрично криптиране (Public Key)



# Модерна криптография

## Асиметрично криптиране (Public Key)





# Модерна криптография

## Асиметрично криптиране (Public Key)

- Pretty Good Privacy (PGP)

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2.0.17 (MingW32)

```
mQMuBFG3x4URCACZ/c7PjmPw0y2qIyKAYRftIT7YurxmZ/wQEwkyLJ4R+A2mFAvw
EfdVjghAKwnXxqeZ09WlyAEofqIX5ewXD9J4H6THaWN1DeNwnIUhbV5SEgT6iwGEG
arXvkrMyy+U5KA0x2dcsYRKAPMM1db+4z5QkTWzUfLU71cKi3gU3pNTxSA0DjCn
wfJQspiyWchSfgZ59+fKaGZJVSE1rS2i2ok5mK3ywCXRWvnAC/VxA3N6T4jvkX/+
1gS/oUgdocP31TeV0L20JH9QgmFYC3jMbErAATo2x9Y8g4NofdvSnntbZk9Giyc
cgOWsa8aFtTjvcBp8hkC13dK5xTZiY0gLsADAQCXSHI7zw4LiNFfCV+Pb09BEqDA
i4JFV/qX7TgfbNX7nwF/fEFu18V161VCsRzeuhMsHHZAQ7PZJfdFhyOubq0fnjkk
2Rdc1eosnP22zP5LoRs1fvIDdL3wnkg1ZUwFICP0HWRzRYcVBaIv9HcqSVBWrIjJ
uscni5QtX3fIU2wqSyP90wquWPk07j0bT0hWihhWPFxiFA6996i/rTZiJH+eFPsw
afxV1RAqH4kaUBen5f5MBBSsf+GkuuQH7gIYQC2k88soPLuFZG5ibDwBqvdUqFG
S39ifnf/2MUx8DrM8bbIPPwIUte1AFVPu7GGzyzAF3yhk/Cdd/YmWlwrwAd4Psev
WpXNSApzSgh/HhY3wVdj9skItQBISXJSVMD4DLvhwAh/Ur5JEgtx5dYgplU/nEr
LGEDUgPeBnewReA8wurAnYeOHGVsu84kXce02tJvnbLn5y1L0dML/u3+59pDXOFR
1TR9QxWd3QIBUY681fa+DiXHSVcfTPz3q+CHMLj7917hfATWwRTemccp6n8a168
tfGXih9t+1Awuq4KuRk0NkGEKrquR3sdGVLdIZ8IteikyYgWcZTYG7oxcj7qpif
ixl0DsI1HXfXQrFVnj0yQuiS8z06+ZuC/8dgi7UBpUkgQLZYosE0fUAdeIAPVgV0
LanXwHRQPD1mBiorge1c1jpbna2K9EyQ1Jbkyn6nkg80aet09brLBMk916mn6mQD
ebQfQ2hyaXMGUGFjaWEGPGN0cGFjaWFAZ21haWwUy29tPoh6BBMRCAAI8QJrt8eF
AhsDBgsJCAcDAgYVCAIJCgsEFgIDAQIeAQIXgAAKCRCA1W2/7nwQXJ/dAP4207se
mHDQZnx14S1rF8AxcCI0DowpBcNwRM8hNHS2QD/TkbCvy4QNq2QNRP26m183eJM
y6PNCcuwsB5TdoLgYq5Ag0EUbfHhRAIAIPrWRsRVTt3nhJ+0dygQJQsywx9wMMX
EL0dpOmWz838kufR02789b5DTRP2qEm+hymfebd42kgam2CLPBt3F6je4ZHP1iaW
BnsihKJBC40ha+b3Wj8UGpH+t6t18voQhQgKK7HNokedMVRQdW3nzBT1p7KbTyLH
pdT+08KUXdh5hMBPrxgPdBB3GFH3QA03hgsWXkZfMHNAX24AG/oimtW5gGLZdvBQ0
wQFfWmsiy+ah8QhoUd1R0UItD6vD9p2I8MAPnheD04E16wdy/An/5k1yoqx8d+pA
ACnoDjpTwR/P2y7Fo05aCXMWz5ZeKobiToXKxRfoaZ1m72FKpLBTI68ABAsH+wet
wHpRPqU9ajhSExUD1d9JL20GyDM+9Mg1q1AQ0U0UOC+OQ51L2bq0tFKI653M7niu
rB7n3bCnSNAYSrtkRDs/YWeuPjaGUcwfngARDIPdzn1rYN87esdavDMBI7hXGjtI
EypYdXyko03Ff1WJtJzKO/5DoLqVcbXmuubXuhDOigLUQroKgxMpXcS1zRuLabPi
m88Jg6uRuZQGtiX95FZkicTh3U6/48D5R56vCfGgJVwDRCTJmxt70hGn9v3bvBQM
uNNuVFD2XS7CQTNxyqCKke5bJdk/XAgFVJ+H15RFgSw+z6I0TumOvHX01LaN1LGV
xEtUdbVSNCE9LoS14f1IYQQYEQgACQUCubfHHQIbDAKCRCA1W2/7nwQXEI4AP49
Se5zeNswzCcaACKa76fh93RK2VW04SfKh3h1WxMVhgD/exv41oZehRIOzNrZjFkQ
uRkFDPE1NWJAngLobMUo93s=
```



# Модерна криптография

## Асиметрично криптиране (Public Key)

- Дигитални подписи (предимство)
  - Оторизация
  - Цялост на данните
  - „Неотхвърлируемост“

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

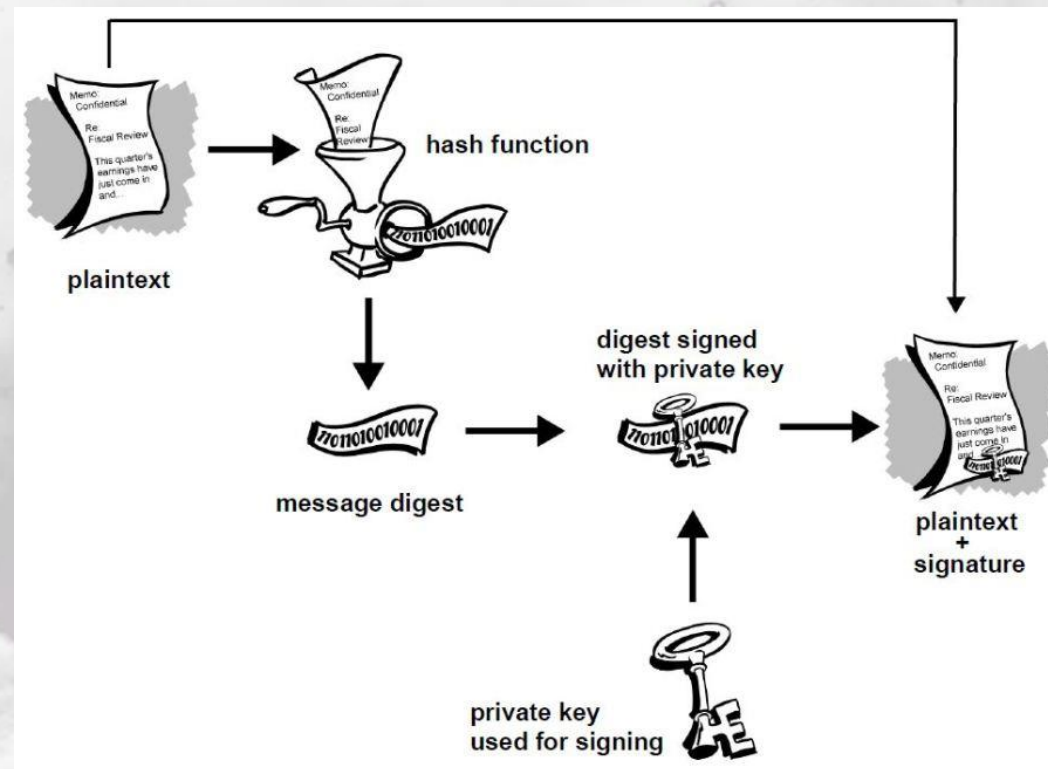
This is an example of a PGP signed message.

-----BEGIN PGP SIGNATURE-----

Version: GnuPG v2.0.17 (MingW32) iF4EAREIAAYFA1IqmD0ACgkQuJVtv+58EFzNTgD/b9tS8CCqnmnKpvR+ZNwr21GP  
bb5Ld3ZLPG/91VJ1udgA/1PI30He1e3F6Dj88wssnrMq0jpSOC+kFuxLnpPZxF83

=p90v

-----END PGP SIGNATURE-----





# Модерна криптография

## Асиметрично криптиране (Public Key)

- Биткойн адрес -> Публична/Частна двойка ключове
- Алгоритъм - Elliptic Curve Digital Signature Algorithm

16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM



# Модерна криптография

## Асиметрично криптиране (Public Key)

*Bitcoin address is technically a base58 encoded RIPEMD160 hash of a SHA-256 hash of **256-bit public key** of an Elliptic Curve Digital Signature Algorithm key pair concatenated with a checksum.*



# Модерна криптография

## Асиметрично криптиране (Public Key)

Фалшифициране на биткойн транзакции не е възможно

- Биткойн – счетоводна книга / баланси
- Транзакцията се подписва с частния ключ
- Сравнява се с публичния ключ от другата страна (страни) (Биткойн адреса)
- Никой не може да създаде валидна транзакция без валиден частен ключ
- Промени по транзакцията инвалидират подписа
- Веднъж щом транзакция е подписана и извършена успешно – никой друг не може да я е извършил



# Модерна криптография

## Криптографски Хеш Функции („копаене“)

Основни характеристики:

- Еднопосочни
  - Лесно: input -> output
  - Трудно (невъзможно): output -> input
- Няма „колизии“ – различни inputs -> еднакви outputs
- Различни по дължина inputs -> еднакви по дължина outputs

1234 ==> 10

```
hello    ==> 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824
goodbye  ==> 82e35a63ceba37e9646434c5dd412ea577147f1e4a41ccde1614253187e3dbf9
```



# Модерна криптография

## Криптографски Хеш Функции („копаене“)

Основни характеристики:

- Малко промяна -> огромна разлика

| Информация                          | Хеш функция                 | Хеш (фиксирана дължина)                              |
|-------------------------------------|-----------------------------|--|
| Fox                                 | cryptographic hash function | DFCD 3454 BBEA 788A 751A<br>696C 24D9 7009 CA99 2D17 |
| The red fox jumps over the blue dog | cryptographic hash function | 0086 46BB FB7D CBE2 823C<br>ACC7 6CD1 90B1 EE6E 3ABC |
| The red fox jumps over the blue dog | cryptographic hash function | 8FD8 7558 7851 4F32 D1C6<br>76B1 79A9 0DA4 AEFE 4819 |
| The red fox jumps over the blue dog | cryptographic hash function | FCD3 7FDB 5AF2 C6FF 915F<br>D401 C0A9 7D9A 46AF FB45 |
| The red fox jumps over the blue dog | cryptographic hash function | 8ACA D682 D588 4C75 4BF4<br>1799 7D88 BCF8 92B9 6A6C |





# Модерна криптография

## Merkle Trees (Дървета на Меркъл)

- Копачите поставят всяка проверена транзакция в „басейн от памет“ (memory pool)
- Всяка транзакция се хешира с хеш функцията SHA256

```
01000000017a06ea98cd40ba2e3288262b28638cec5337c1456aaf5eedc8e9e5a20f062bdf000000008a473044022030e2d2  
3be71a907a3ad7de846b3bbe8886c4a839e1aa2cf0d314b1d327f12d2a022039718fc3886a171e4ec2b138e6547b03dd326e  
f7f12295d06e351e7c02010068014104e0ba531dc5d2ad13e2178196ade1a23989088cfbeddc7886528412087f4bffa2ebc19  
ce739f25a63056b6026a269987fcf5383131440501b583bab70a7254b09efffffffffff01b02e052a010000001976a9142dbde3  
0815faee5bf221d6688ebad7e12f7b2b1a88ac00000000
```



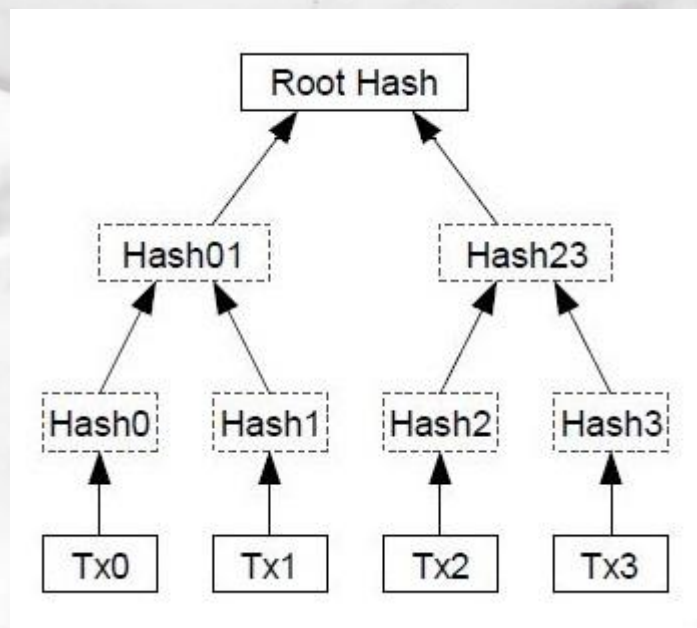
```
2d94683fa2f8aaaae4a6f377d93b875f680adf96b9c3e9577554b742f412fa9ad
```



# Модерна криптография

## Merkle Trees (Дървета на Меркъл)

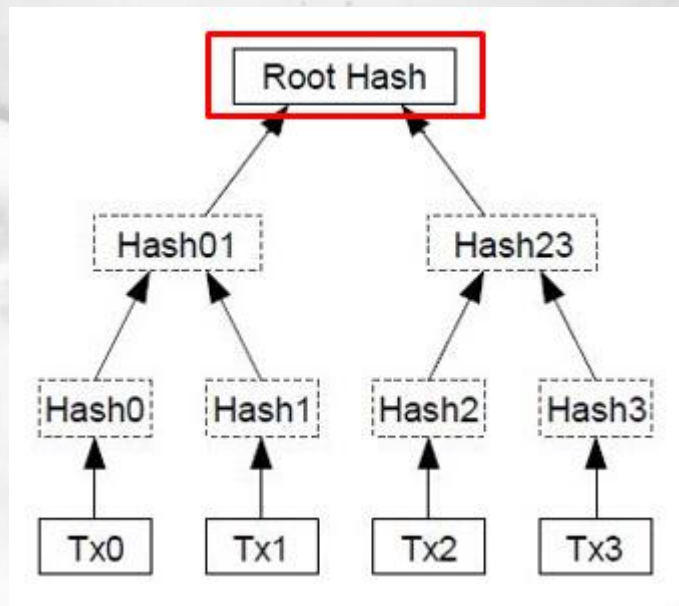
- Всяка двойка транзакции се хешира отново
- Получава се (обърнато) дърво от хеширани транзакции



# Модерна криптография

## Merkle Trees (Дървета на Меркъл)

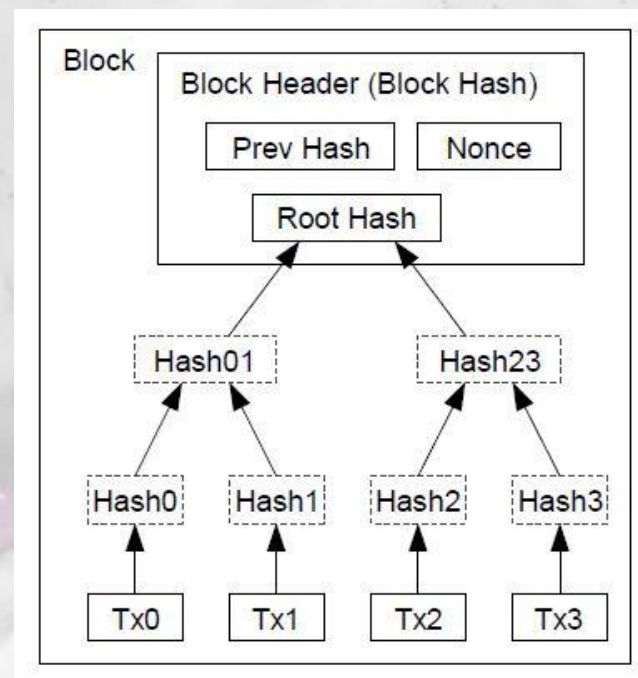
- Хешът най-отгоре -> Корен на хеша (Root Hash)



# Модерна криптография

## Merkle Trees (Дървета на Меркъл)

- Коренът на настоящия блок + коренът на предходния блок + nonce (произволно число)
- „Заглавие на блока“ (Block Header / Block Hash)
- Заглавието се хешира с SHA256





# Модерна криптография

## Доказателство за свършена работа (Proof of Work)

- Хешираното заглавие на блока – трябва да започва с определено количество нули!

```
0000000000000002e9067f1cf7252333f7aeb619c89d220985a70ac0e015248e0
```

- Минава се през цялата процедура на хеширане и накрая се получава хеш
- Ако не отговаря на условията – променя се nonce-a (произволното число)

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfd65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```





# Модерна криптография

## Доказателство за свършена работа (Proof of Work)

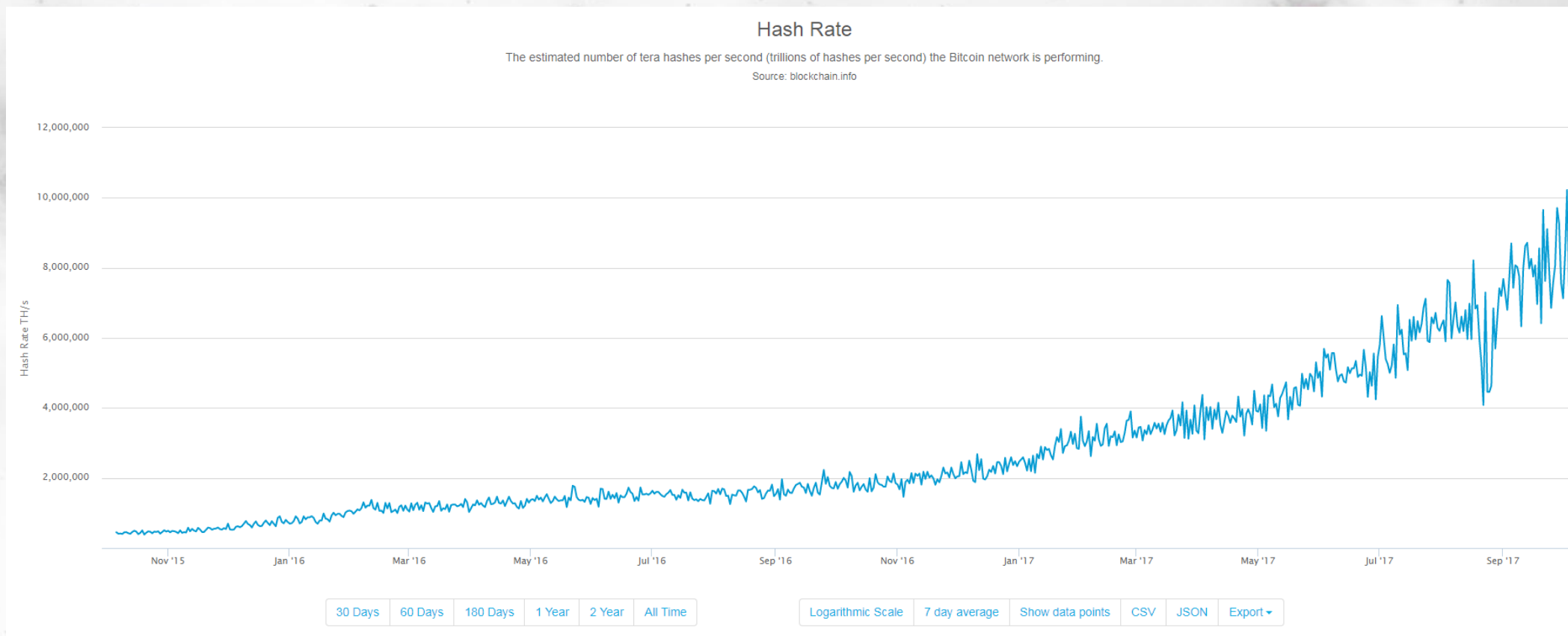
### Block #488275

| Summary                      |                      | Hashes         |  |
|------------------------------|----------------------|----------------|--|
| Number Of Transactions       | 2182                 | Hash           | 00000000000000000aebd4d821ad8ee2ef30c4aacc7619ce309d8570f7fb9b   |
| Output Total                 | € 44,216,933.33      | Previous Block | 0000000000000000002883a86000c028a2eafe0a4019e5f710a6e3e0f9d4daa  |
| Estimated Transaction Volume | € 2,664,978.66       | Next Block(s)  |  |
| Transaction Fees             | € 4,758.14           | Merkle Root    | a2fdc6d05fe5ce070fffc2db60c1e2686cc21543becebca8bb3ba8e0294f23e8 |
| Height                       | 488275 (Main Chain)  |                |  |
| Timestamp                    | 2017-10-04 11:37:58  |                |  |
| Received Time                | 2017-10-04 11:37:58  |                |  |
| Relayed By                   | AntPool              |                |  |
| Difficulty                   | 1,123,863,285,132.97 |                |  |
| Bits                         | 402717299            |                |  |
| Size                         | 999.133 kB           |                |  |
| Weight                       | 3844.159 kWU         |                |  |
| Version                      | 0x20000000           |                |  |
| Nonce                        | 2666439628           |                |  |
| Block Reward                 | € 45,166.50          |                |  |



# Модерна криптография

## Доказателство за свършена работа (Proof of Work)



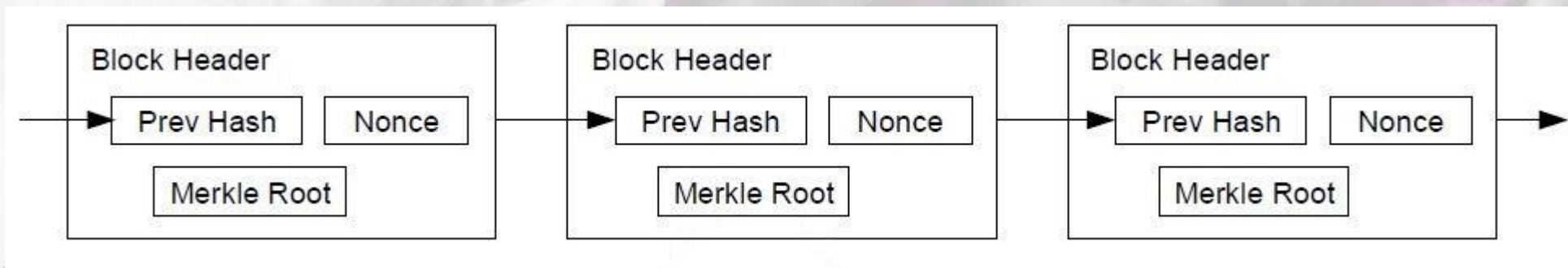
10 000 000 000 000 000 000 000 H/s (exa)



# Модерна криптография

## Доказателство за свършена работа (Proof of Work)

- Всеки блок е криптографски свърза с предходния блок
- Промяната дори на една транзакция оказва влияние върху корена на блока
- От там – и на заглавието на блока

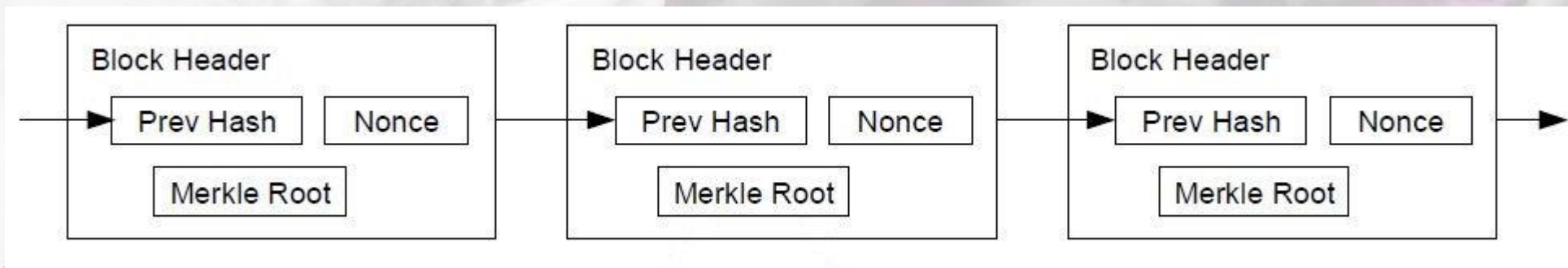


# Модерна криптография

## Доказателство за свършена работа (Proof of Work)

- Промяна на дори 1 транзакция изисква:
  - Ре-хеширане на валидно заглавие (0000000...)
  - Хеширане на валидно заглавие на всеки следващ блок
  - Мрежата ще е по-бърза от скоростта на атакуващия (>51%)
  - Блокове във валидната мрежа ще се намират по-бързо
  - Най-дългата верига от блокове се счита за валидна

```
q=0.1
z=0 P=1.0000000
z=1 P=0.2045873
z=2 P=0.0509779
z=3 P=0.0131722
z=4 P=0.0034552
z=5 P=0.0009137
z=6 P=0.0002428
z=7 P=0.0000647
z=8 P=0.0000173
z=9 P=0.0000046
z=10 P=0.0000012
```



# Модерна криптография

## Заключение

- Увеличаване на възможните комбинации
- Премахване на възможности за дедукция
- Не е важно дали може да се дешифрира, а колко време ще отнеме

## Биткойн

- Симфония на криптографията
- Защитен от математически закони вече 8 години
- „Криптовалути“ -> защита на информация „кой какво притежава“ чрез криптография







vlad@aeternity.com

[www.aeternity.com](http://www.aeternity.com)

