Введение в криптографию

Симметричное шифрование

Классические шифры

Кому и зачем нужно шифрование?

Что такое …?

Шифрование — обратимое преобразование информации в целях скрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней.

Расшифрование - процесс преобразования зашифрованных данных в открытые данные при помощи ключа.

Дешифрование - процесс преобразования зашифрованных данных в открытые данные без ключа.

Базовые понятия

Открытый текст (plaintext)

- Исходное сообщение

Ключ (key)

- Секретный параметр

Шифротекст (ciphertext)

- Зашифрованное сообщение

Шесть требований Керкгоффса

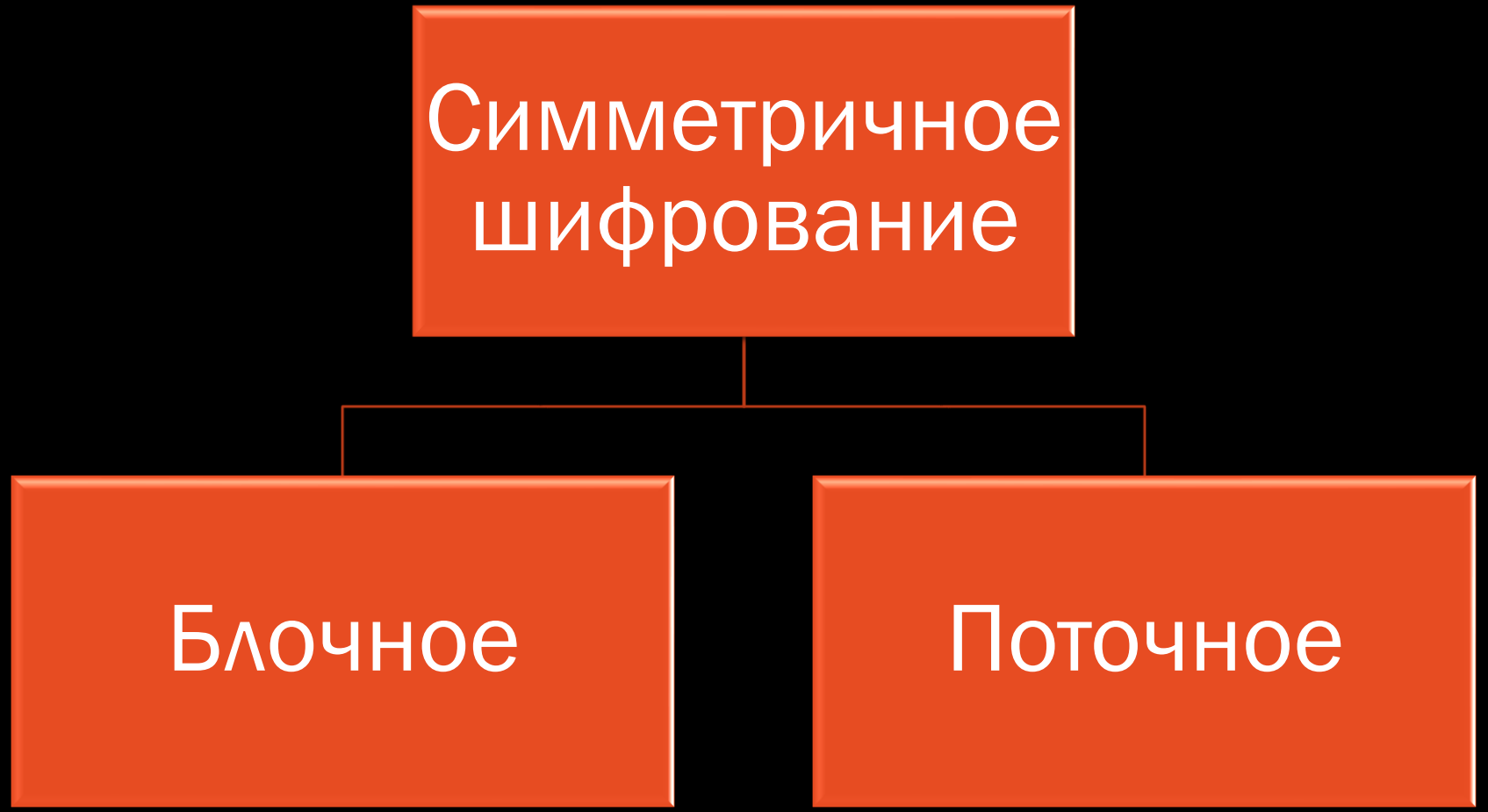
- Система должна быть физически, если не математически, невскрываемой;
- Нужно, чтобы не требовалось сохранение системы в тайне; попадание системы в руки врага не должно причинять неудобств; (принцип Керхгоффса)
- Хранение и передача ключа должны быть осуществимы без помощи бумажных записей; корреспонденты должны располагать возможностью менять ключ по своему усмотрению;

Шесть требований Керкгоффса

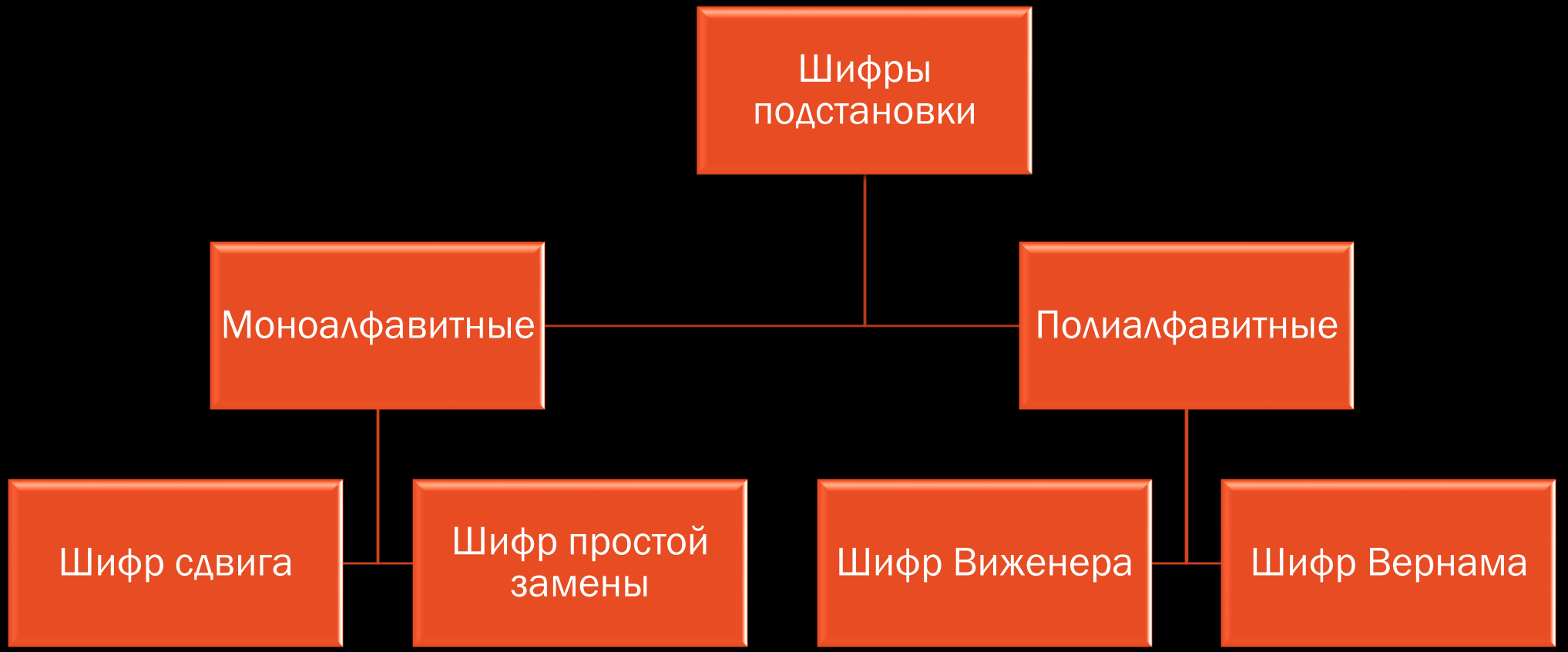
- Система должна быть пригодной для сообщения через телеграф;
- Система должна быть легко переносимой, работа с ней не должна требовать участия нескольких лиц одновременно;
- Наконец, от системы требуется, учитывая возможные обстоятельства её применения, чтобы она была проста в использовании, не требовала значительного умственного напряжения или соблюдения большого количества правил.

Шифрование бывает…

- Симметричным (ключ расшифрования совпадает с ключом шифрования, либо же легко находится из него)
- Асимметричным (имеется пара ключей – приватный и публичный, приватный держится в секрете, через публичный ключ вычислить сложно)


Симметричное шифрование
Блочное
Поточное


Симметричное шифрование
Шифры подстановки (замены)
Перестановочные (транспозиционные) шифры
Смешанное


Шифры подстановки
Моноалфавитные
Полиалфавитные
Шифр сдвига
Шифр простой замены
Шифр Виженера
Шифр Вернама

Шифр Цезаря (Caesar cipher)

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
D	E	F	G	H	I	J	K	L	M	N	O	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D

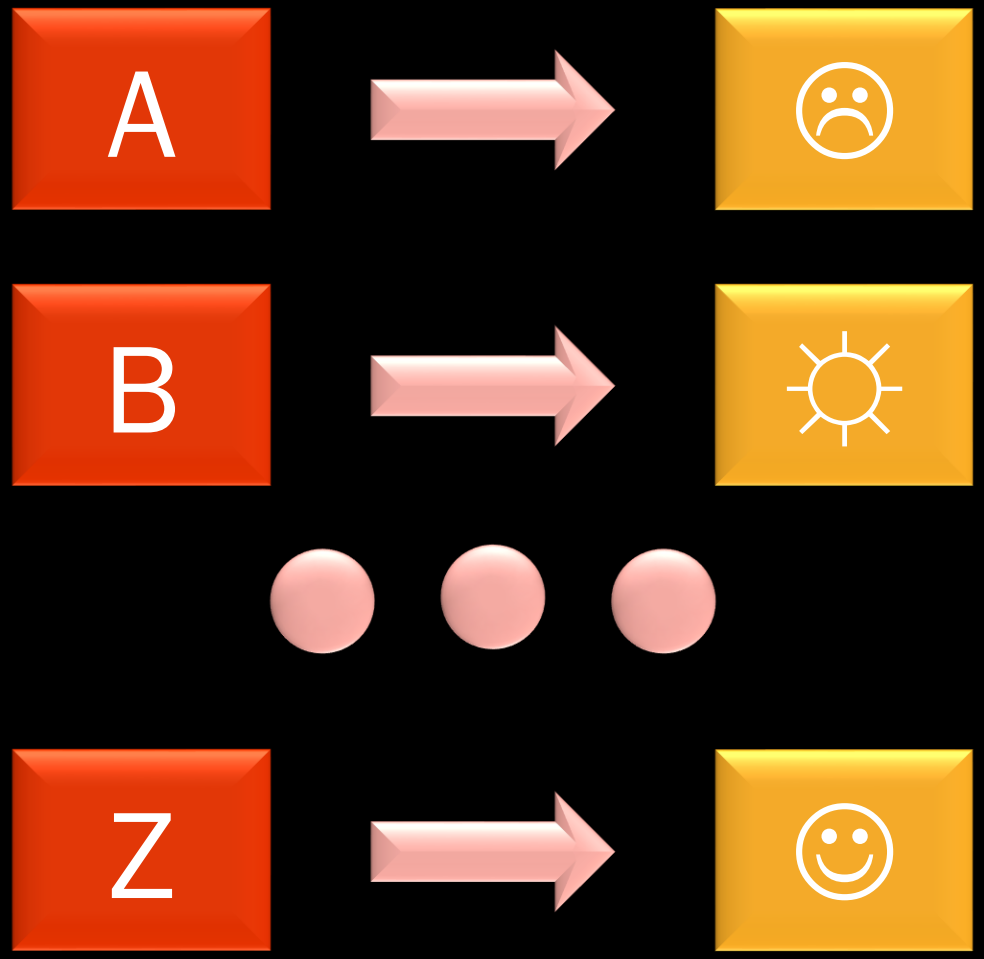
- Пример:

EASY CRYPTO
HDVB FUBSWR

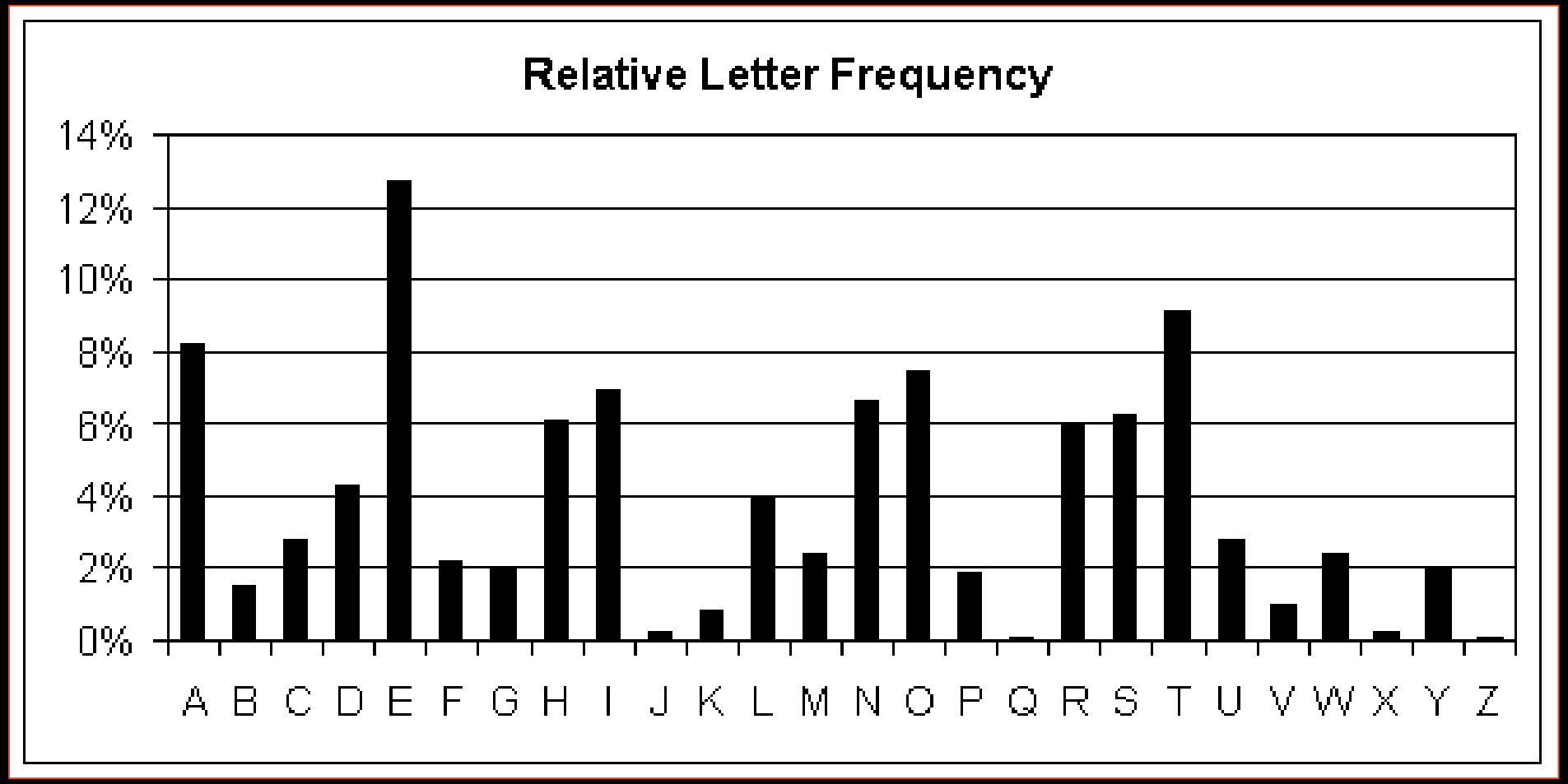
Шифр сдвига

- $C_i = (M_i + k)\ mod\ |A|$,
- $M_i = (|A| + C_i - k)\ mod\ |A|$,
  - C_i (M_i) – буква с i-ой позицией в шифротексте (сообщении)
  - k – ключ сдвига
  - $|A|$ - мощность алфавита
  - Пример: Шифр Цезаря. Ключ 3

Шифр простой замены



Частотный анализ



Шифр Виженера (Vigenere Cipher)

- *Ключом является слово (фраза)*

- $C_i = (M_i + k_{i \bmod n}) \bmod |A|$,
- $M_i = (|A| + C_i - k_{i \bmod n}) \bmod |A|$,
  - C_i (M_i) – буква с i-ой позицией в шифротексте (сообщении)
  - $k_{i \bmod n}$ – буква с i-ой позицией в ключе с циклическим сдвигом относительно длины ключа n
  - $|A|$ - мощность алфавита

Шифр Вернама (одноразовый блокнот, One Time Pad)

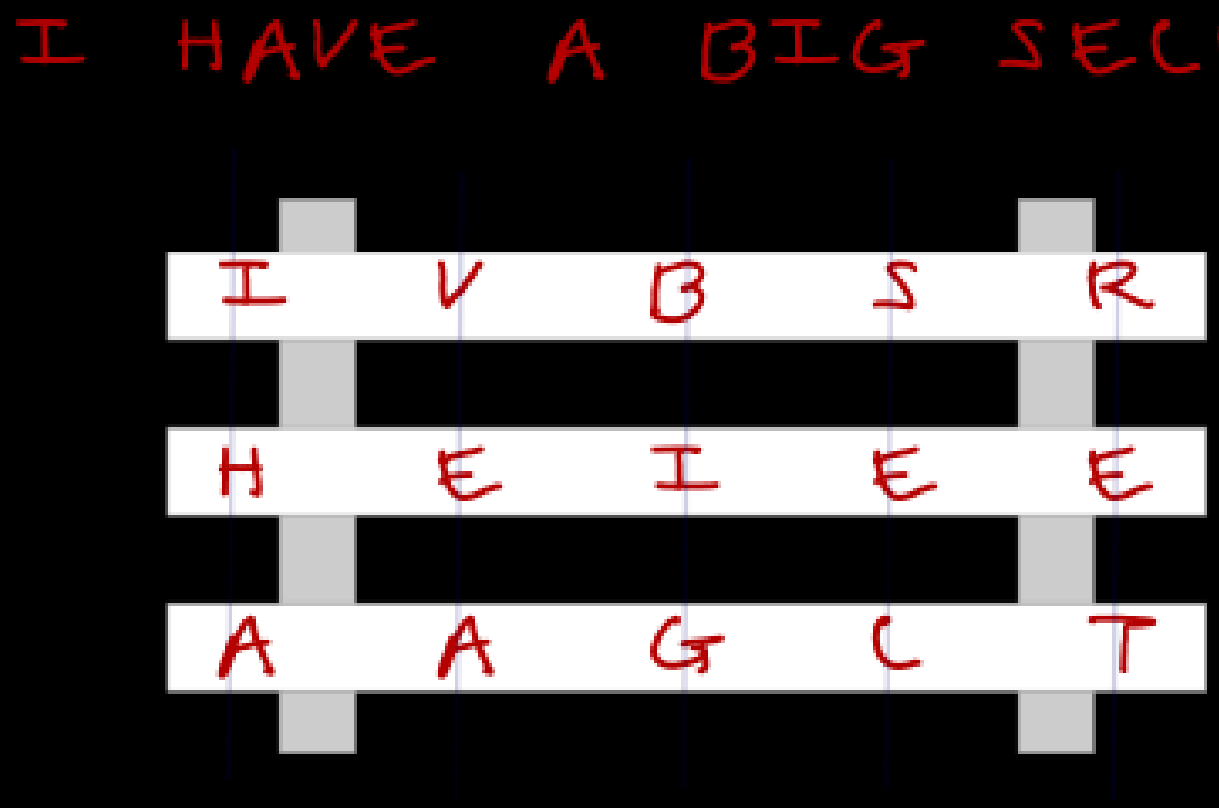
- *Длина ключа равна длине сообщения*
- *Ключ случаен*

- $C_i = (M_i + k_i)\ mod\ |A|$,
- $M_i = (|A| + C_i - k_i)\ mod\ |A|$,
  - C_i (M_i) – буква с i-ой позицией в шифротексте (сообщении)
  - k_i – буква с i-ой позицией в ключе
  - $|A|$ - мощность алфавита

Сцитала (скитала)

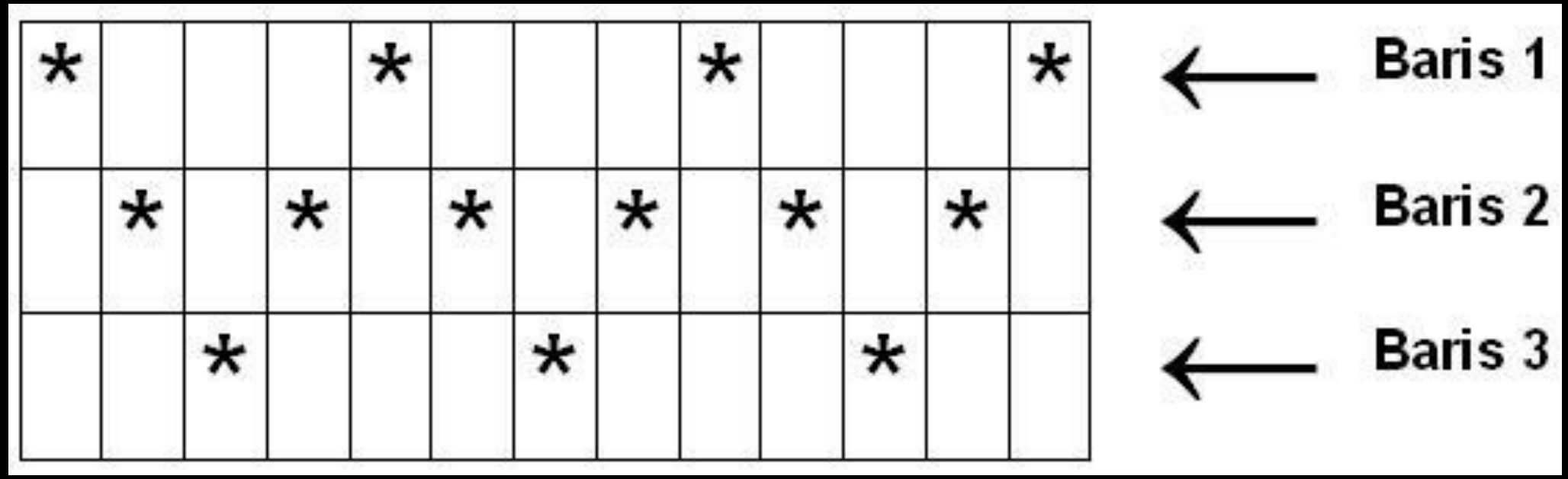
Сцитала (скитала)

- Plaintext: IHAVEABIGSECRET
- Ciphertext: IVBSRHEIEEAAGT



Ключ: 3

Rail Fence Cipher (Zig-Zag)



Rail Fence Cipher (Zig-Zag)

Plaintext: PLEASE HELP ME NOW.

P H N

L E E E O

E S L M W

A P

Ciphertext: PHNLE EEOES LMWAP

Ключ: 4