Математические и компьютерные основы защиты информации

Лекция 1

Антон Николаевич Гайдук | УНИВЕР

vk.com/gaidukedu

09 февраля 2023 г.

Объем дисциплины

ЯНВАРЬ

ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

ФЕВРАЛЬ

ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28					

МАРТ

ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31		

АПРЕЛЬ

ПН	ВТ	СР	ЧТ	ПТ	СБ	ВС
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

- Лекции — один раз в неделю (всего 9)
- Практические занятия — один раз в неделю (всего 7)

Отчетность

- защита отчета по лабораторным работам
- зачет

Литература

Криптология : учебник / Ю. С. Харин [и др.]. - Минск: БГУ, 2013. -511 с. - (Классическое университетское издание). https://elib.bsu.by/handle/123456789/259637

Харин Ю. С. Компьютерный практикум по математическим методам защиты информации: Учеб. пособие / Ю. С. Харин. С. В. Агиевич. - Мн.: БГУ, 2001. - 190 с..

Криптографические методы. С.В. Агиевич. – 2014. http://apmi.bsu.by/assets/files/agievich/cm.pdf

Содержание дисциплины

Раздел I Введение

- Тема 1. Введение. История. Основные понятия.

Раздел II Симметричная криптография

- Тема 2 Классические шифры.
- Тема 3 Поточные алгоритмы шифрования.
- Тема 4 Блочные алгоритмы шифрования.

- Тема 5 Функции хэширования.
- Тема 6 Математические методы криптоанализа.

Раздел III Асимметричная криптография

- Тема 7 Протокол Диффи-Хэллмана.
- Тема 8 Криптосистемы с открытым ключом.
- Тема 9 Электронная цифровая подпись.

Тема 1. Введение

Методы защиты информации

- Правовые
- Организационные
- Технические
- Стеганографические
- Криптографические

Криптогра́фия (от др.-греч. κρυπτός «скрытый» + γράφω «пишу»)

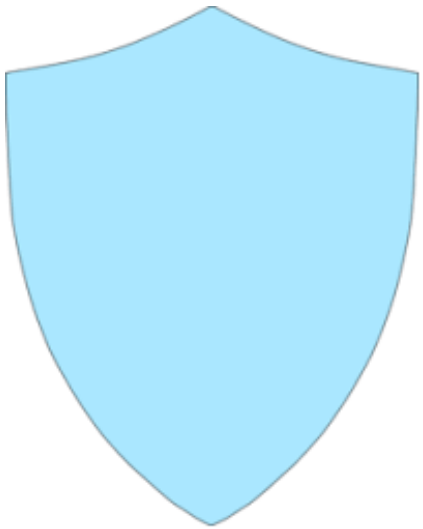
В отличии от других способов защиты информации криптографические методы основаны на математических и компьютерных преобразованиях защищаемой информации.

Примеры использования криптографии

Примеры использования криптографии



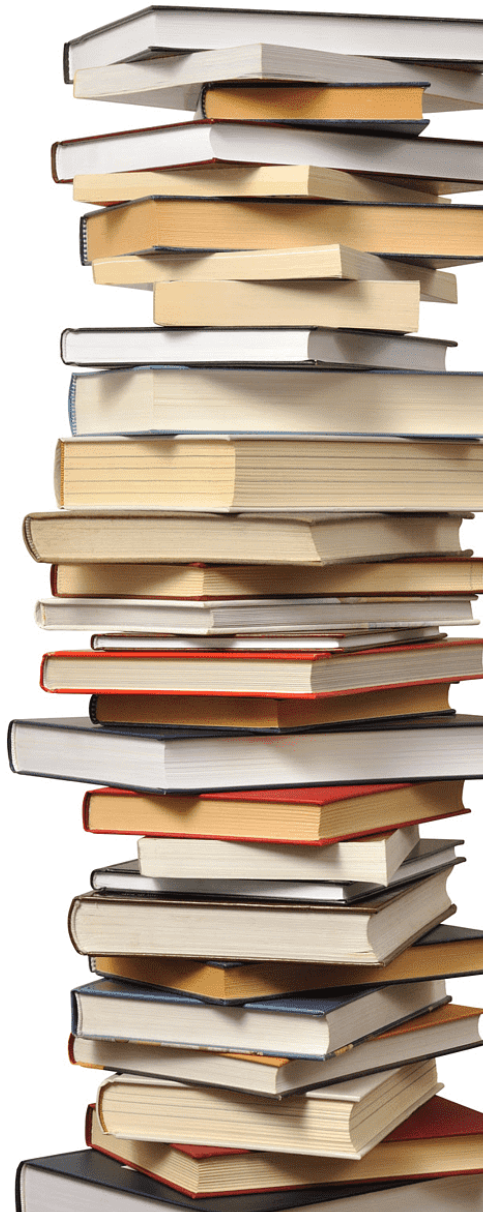

Криптология



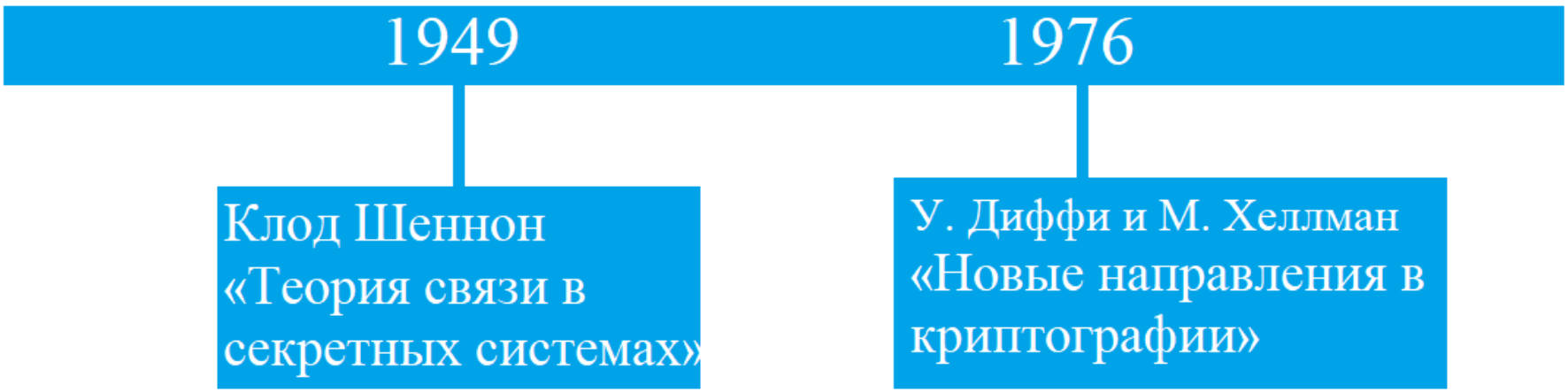
Криптология = криптография и криптоанализ.

Современная криптология на стыке наук

- Теория множеств
- Теория чисел
- Дискретная математика
- Алгебра
- Теория информации
- Теория вероятностей
- Математическая статистика
- Математическое моделирование
- Теория алгоритмов
- Теория вычислимости
- Физика



История


1949
1976
Клод Шеннон «Теория связи в секретных системах»
У. Диффи и М. Хеллман «Новые направления в криптографии»

Шифр Атбаш

- Шифр простой подстановки (замены)
- Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.
- Впервые встречается в древнееврейском тексте Библии / Танаха.

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

אתבש (атбаш на иврите)

א - «алеф» (1-я буква еврейского алфавита),
ת - «тав» (последняя буква еврейского алфавита),
ב - «бет» (2-я буква еврейского алфавита),
ש - «шин» (предпоследняя буква еврейского алфавита)

История криптографии: античность

Скитала (от греч. жезл)

- перестановочное шифрование
- секретный параметр шифра — диаметр цилиндра

Пример

ЭТОШИФРДРЕВНЕЙСПАРТЫ

Э	Т	О	Ш	И
Ф	Р	Д	Р	Е
В	Н	Е	Й	С
П	А	Р	Т	Ы

ЭФВПТРНАОДЕРШРЙТИЕСЫ

История криптографии: античность

Шифр Цезаря

- шифр простой подстановки (замены)
- секретный параметр шифра — величина сдвига

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	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Пример

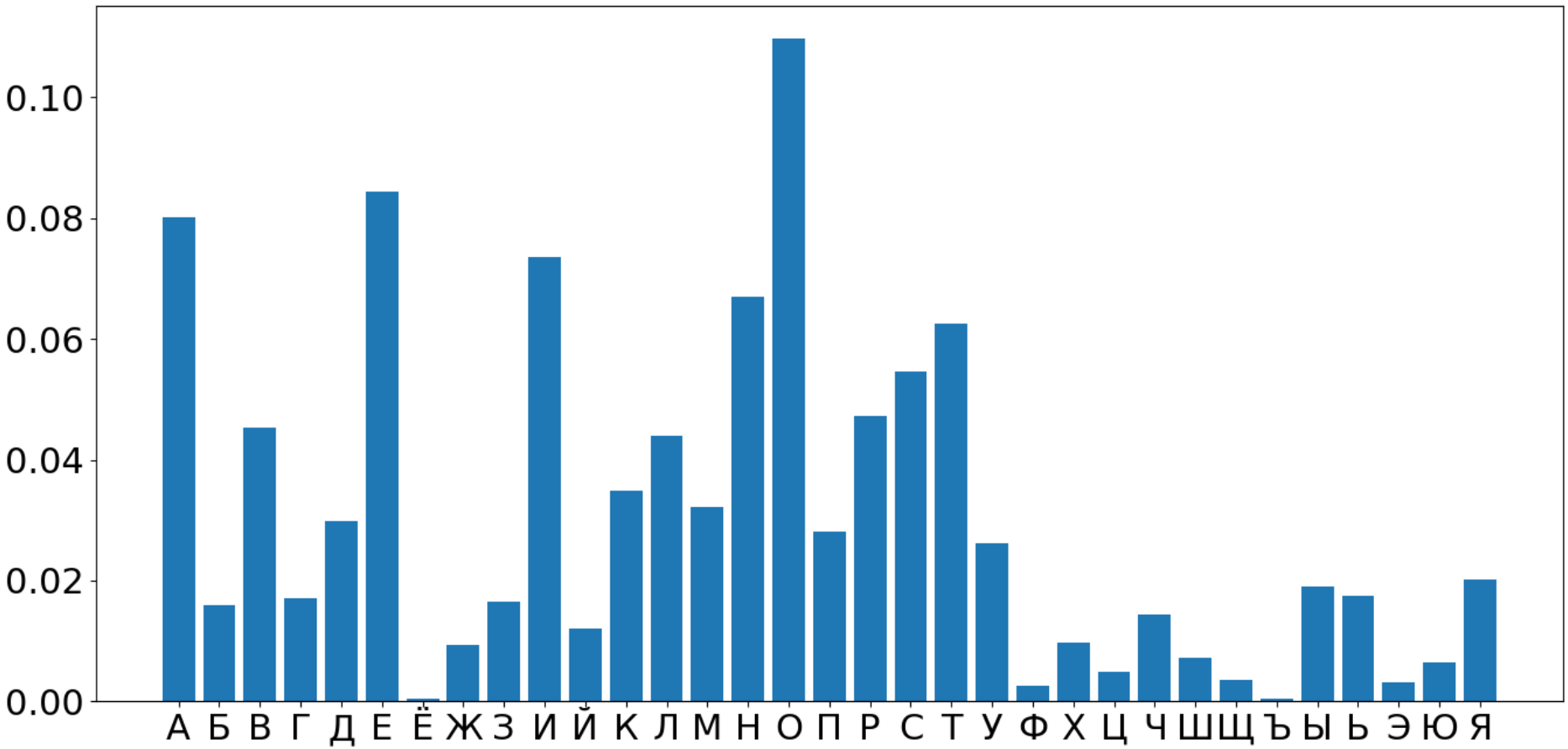
YLYDW VWXGHQW $\longrightarrow$ VIVAT STUDENT

Способности к криптоанализу есть у каждого :)

По рзелульаттам илссеовадний одонго анлигйсокго унвиертисета, не иеемт занчнеия, в кокам пряокде рсапожолены бкувы в солве. Галвоне, чотбы преавя и пслоендяя бквуы блыи на мсете. Осатьлыне бкувы мгоут селдовтаь в плоонм бсепордяке, все-рвано ткест чтаитсея без побрелм. Пичрионй эгото ялвятеся то, что мы не чиатем кдаужю бкуву по отдльенотси, а все солво цликеом.

История криптографии: античность

- Характеризуется господством моноалфавитных шифров, основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами.
- Основная уязвимость — частотный криптоанализ.



История криптографии: эпоха Возрождения и новое время

- Появление омофонов – шифров многозначной замены: каждой букве ставится в соответствие несколько эквивалентов, число которых пропорционально частоте встречаемости этой буквы
- Появление многоалфавитных шифров.

Диск Альберти

Шифр Виженера

- многоалфавитный шифр
- секретный параметр шифра — ключевое слово

Пример (ключевое слово: MINSK)

V	I	V	A	T	S	T	U	D	E	N	T
M	I	N	S	K	M	I	N	S	K	M	I
H	Q	I	S	D	E	B	H	V	O	Z	B

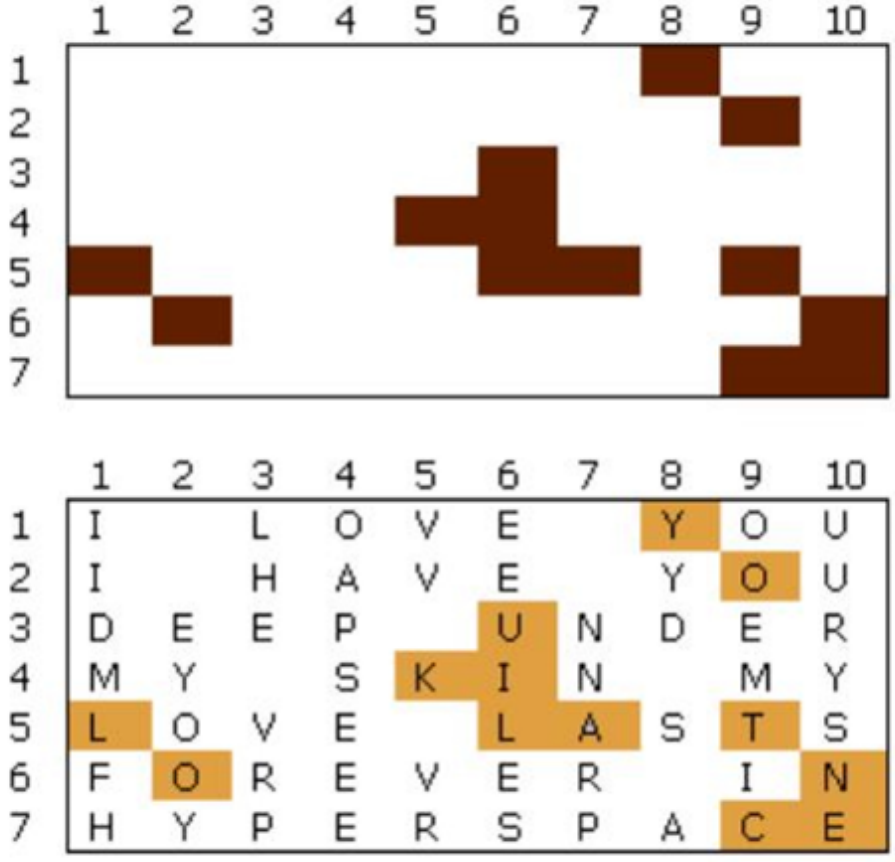
Криптоанализ

- тест Касиски
- индекс Фридмана (индекс совпадений)

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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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
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

Шифр Кардано и Ришелье

- шифровальная решетка
- секретный параметр шифра — трафарет с прорезями-ячейками



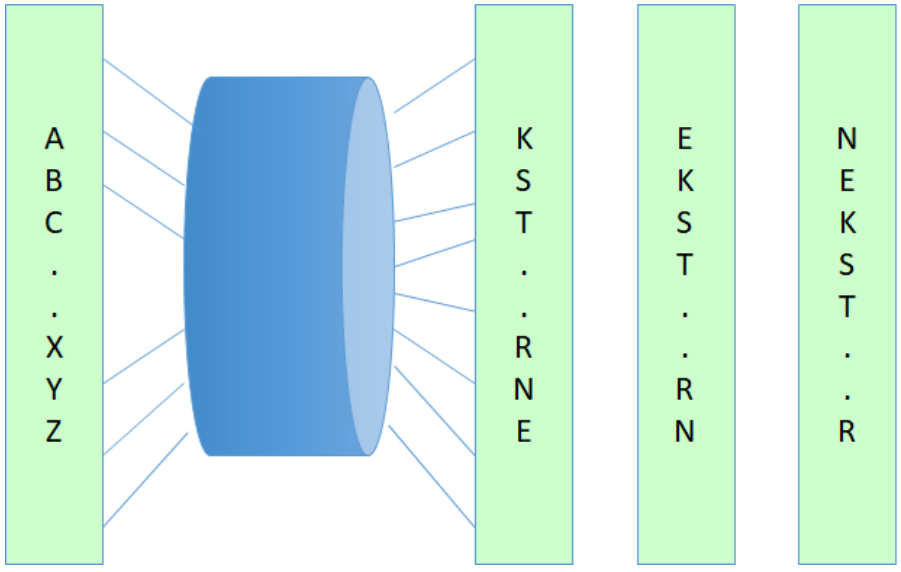
История криптографии: (конец XVIII в.)

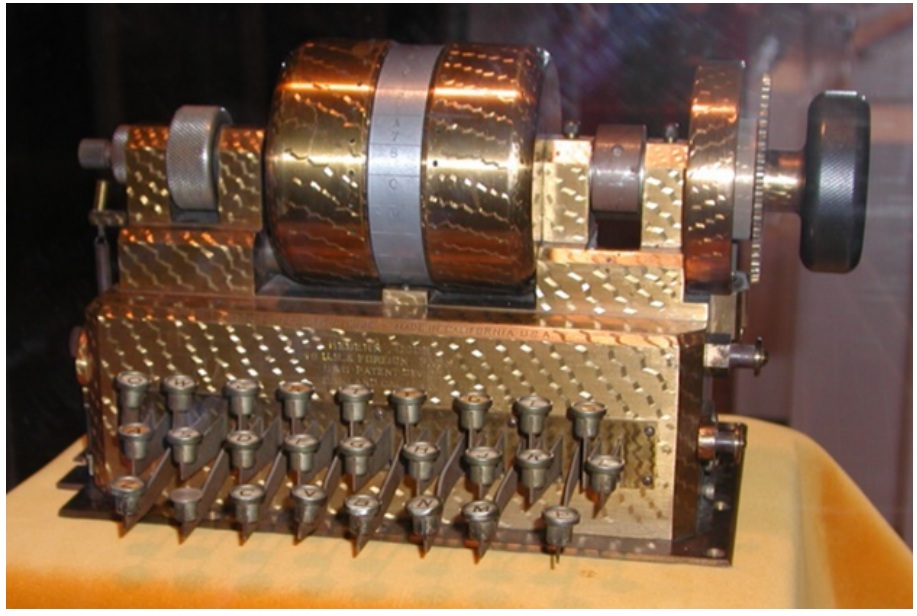
Шифратор Джефферсона

- шифр многоалфавитной замены
- секретный параметр шифра — порядок расположения букв на каждом из дисков и порядок дисков на оси (всего 36 дисков)

Шифратор Хеберна

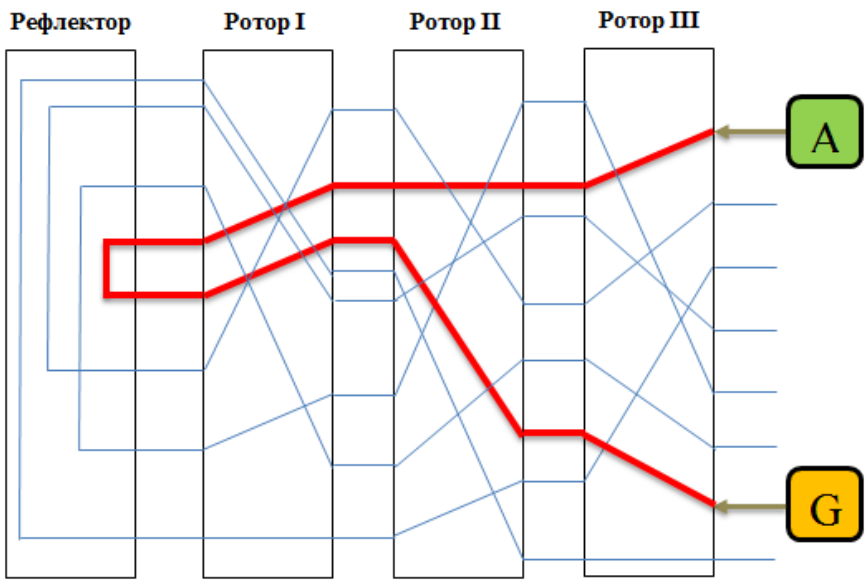
- шифр многоалфавитной замены: роторный шифратор
- секретный параметр шифра — порядок расположения букв на диске





Энигма

- шифр многоалфавитной замены: роторный шифратор
- секретный параметр шифра — диски, порядок расположения дисков



Шифр Вернама (одноразовый блокнот)

- шифр с абсолютной криптографической стойкостью
- секретный параметр шифра — ключ такой же длины, что и сообщение

Пример

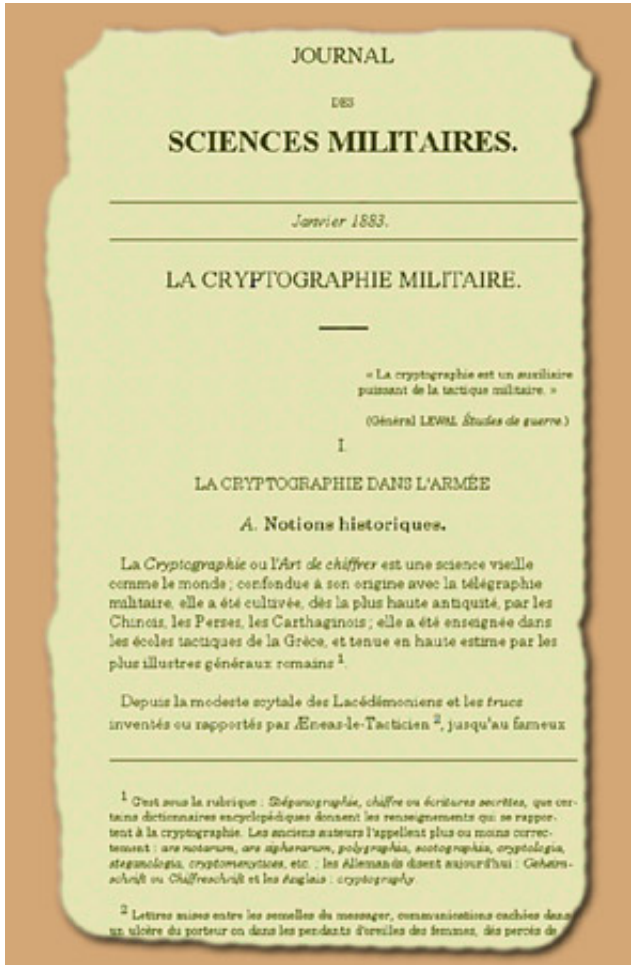
$$\begin{array}{cccccccc} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ \hline 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \end{array} \quad (\oplus)$$

Принципы Керкхоффса

Принцип Керкхоффса — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм предполагается известным.

Книга «Военная криптография»

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



JOURNAL

DES

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire puissant de la tactique militaire. »

(Général LEWAL *Études de guerre.*)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. **Notions historiques.**

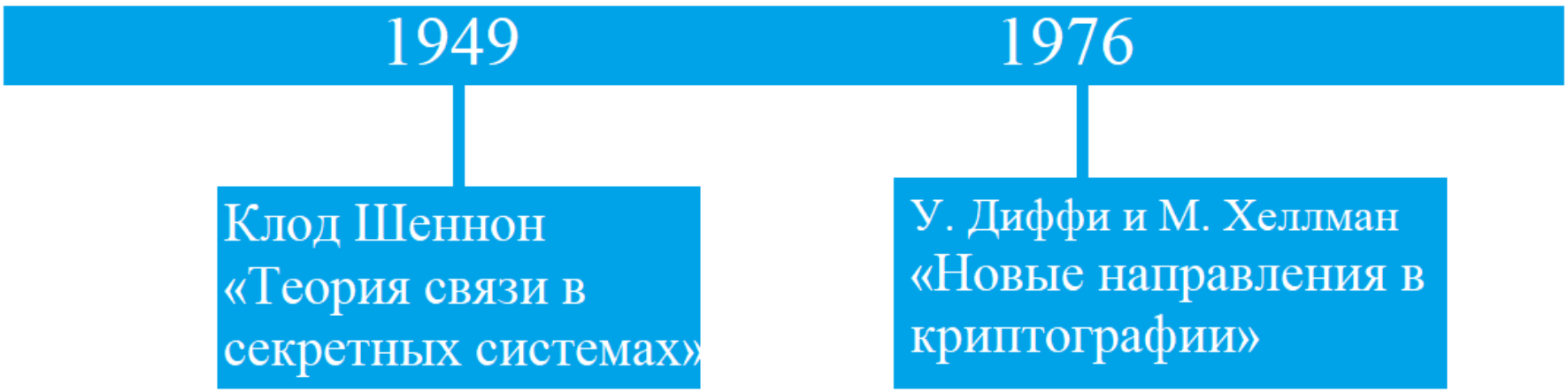
La *Cryptographie* ou l'*Art de chiffrer* est une science vieille comme le monde ; confondue à son origine avec la télégraphie militaire, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle a été enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les plus illustres généraux romains [1].

Depuis la modeste scytale des Lacédémoniens et les *truces* inventés ou rapportés par Æneas-le-Tacticien [2], jusqu'au fameux

[1] C'est sous la rubrique : *Stéganographie, chiffre ou écritures secrètes*, que certains dictionnaires encyclopédiques donnent les renseignements qui se rapportent à la cryptographie. Les anciens auteurs l'appellent plus ou moins correctement : *ars notarum, ars alphanum, polygraphia, scotographia, cryptologia, steganologia, cryptomenytices*, etc. ; les Allemands disent aujourd'hui : *Geheimschrift* ou *Chiffrenschrift* et les Anglais : *cryptography*.

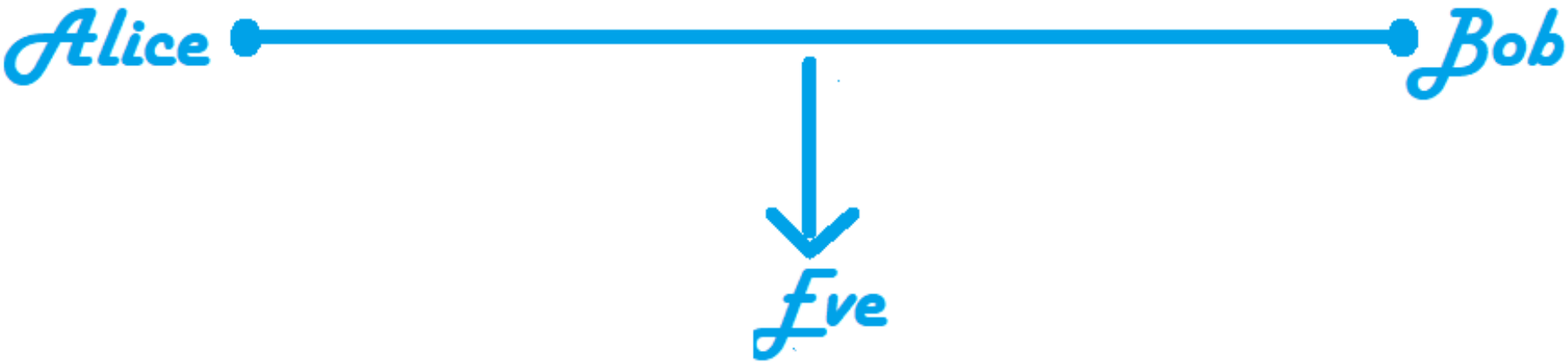
[2] Lettres mises entre les semelles du messager, communications cachées dans la ulotte du porteur ou dans les pendants d'oreilles des femmes, dès percés de

История

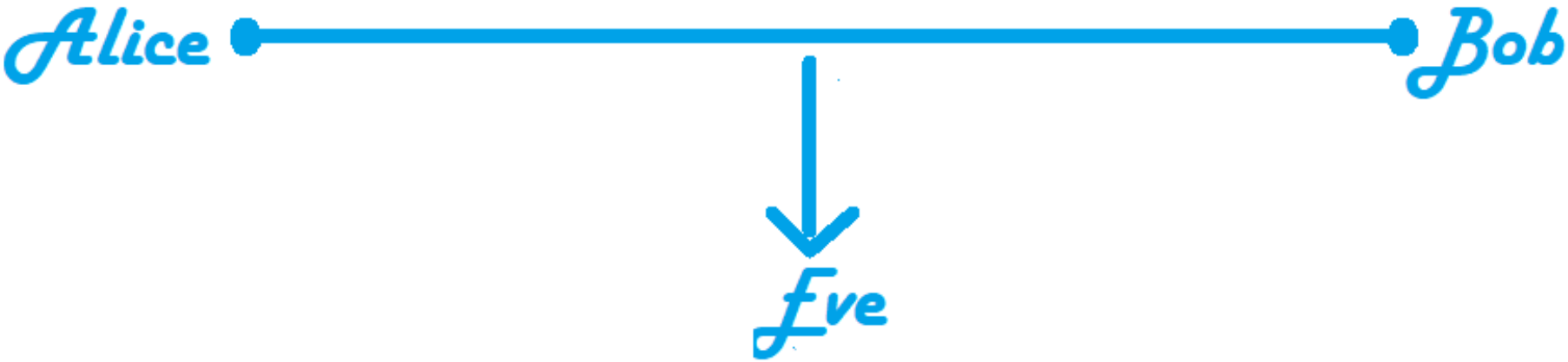

1949
1976
Клод Шеннон «Теория связи в секретных системах»
У. Диффи и М. Хеллман «Новые направления в криптографии»

Основные понятия

Общепринятые имена участников

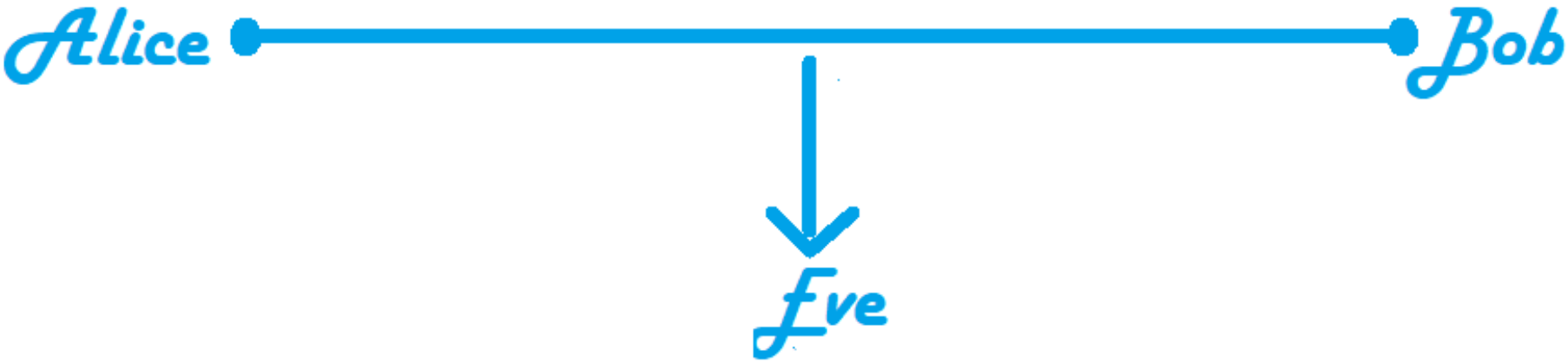


Общепринятые имена участников



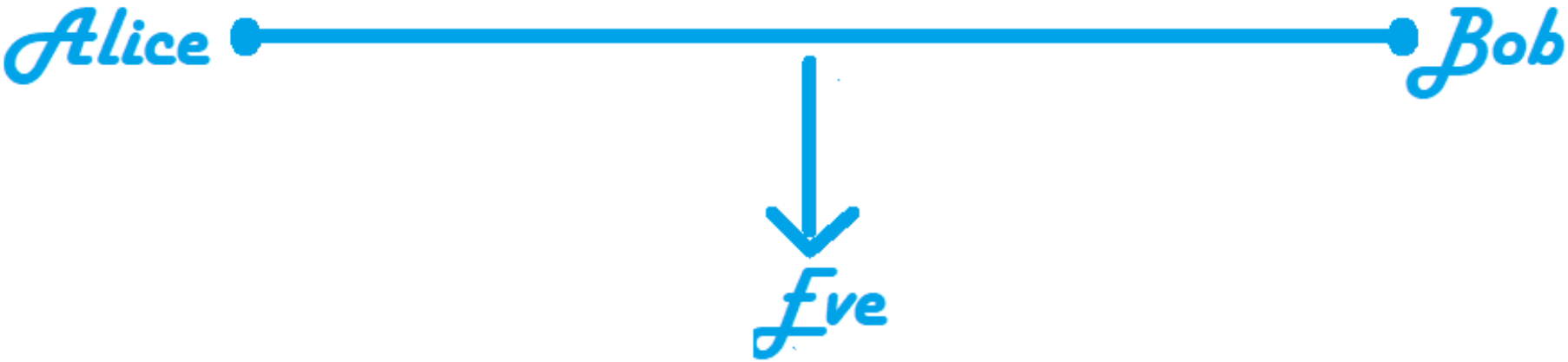
- Алиса и Боб обмениваются сообщениями
- Ева перехватывает сообщения (нарушение конфиденциальности)

Общепринятые имена участников



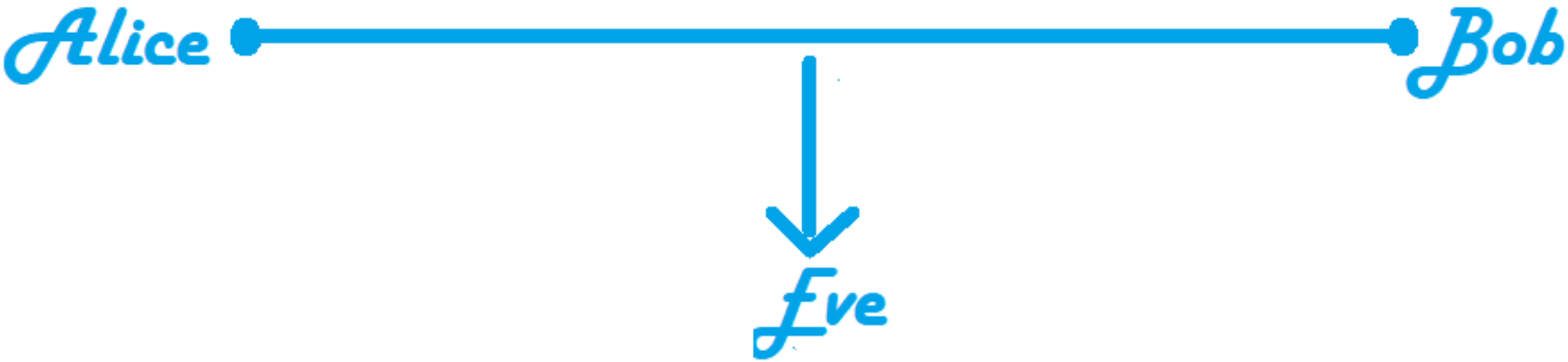
Обеспечение конфиденциальности информации — защита информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней

Общепринятые имена участников



- Исходное сообщение Алисы называется **открытым текстом**
- Алиса шифрует или **зашифровывает** (encrypt) открытый текст и получает **шифртекст**
- Боб **расшифровывает** (decrypt) шифртекст
- Ева перехватывает и пытается **дешифровать** (decrypt) шифртекст (выполняет атаку)

Общепринятые имена участников



Способность криптографического алгоритма противостоять атакам называется (крипто)стойкостью

Симметричное и асимметричное шифрование

Математическая модель симметричной шифрсистемы

Определение

Шифрсистемой называется пятерка $\{\mathcal{K}, \mathcal{P}, \mathcal{C}, E, D\}$, где
$\mathcal{K}$ — множество ключей (секретных параметров),
$\mathcal{P}$ — множество открытых текстов,
$\mathcal{C}$ — множество шифртекстов,
E — семейство преобразований зашифрования $E = \{E_k : \mathcal{P} \to \mathcal{C} | k \in \mathcal{K}\}$
D — семейство преобразований расшифрования $D = \{D_k : \mathcal{C} \to \mathcal{P} | k \in \mathcal{K}\}$
с ограничениями

- однозначность расшифрования: $D_k(E_k(p)) = p$ для $\forall p \in \mathcal{P}$;
- реализуемость всех шифртекстов: $\bigcup\limits_{k \in \mathcal{K}} \bigcup\limits_{p \in \mathcal{P}} E_k(p) = \mathcal{C}$, т.е.

  $\forall c \in \mathcal{C} \qquad \exists p \in \mathcal{P}, k \in \mathcal{K}$ такие, что $E_k(p) = c$.

Математическая модель симметричной шифрсистемы

Пусть A — некоторый конечный алфавит, например:
$A = \{0, 1\}, A = \{0, 1, \ldots, 25\}, A = \{0, 1, \ldots, 255\}$.

Через $A^n = \prod_{i=1}^{n} A$ обозначим множество всех слов длины n из алфавита A:

$$A^n = \{a_1 \ldots a_n | a_i \in A, n \geqslant 1 \text{ и } i = \overline{1, n}\}$$

Через $A^* = \bigcup_{i=0}^{\infty} A^i$ обозначим множество всех слов конечной длины.

Классификация симметричных шифрсистем

Поточные алгоритмы шифрования

По ключу $k \in \mathcal{K}$ строится последовательность $\gamma_1 \dots \gamma_n$ шифрование открытого текста $p = p_1 \dots p_n$ осуществляется посимвольно:

$$p = p_1 \dots p_n \to E_{\gamma_1}(p_1) \dots E_{\gamma_n}(p_n) = c_1 \dots c_n = c,$$

$p_i \in A, c_i \in A, i = \overline{1, n}.$

Блочные алгоритмы шифрования (режим ECB)

Шифрование осуществляется блоками некоторой длины L

$$p = p_1 \dots p_m \to E_k(p_1) \dots E_k(p_m) = c_1 \dots c_m = c,$$

$p_i \in A^L, c_i \in A^L, i = \overline{1, n}.$

Спасибо за внимание :)