

# CRYPTOGRAPHY



---

## МЕТОДИ ТА ЗАСОБИ КРИПТОГРАФІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

**Башков Євген Олександрович, д.т.н., проф.,  
кафедра прикладної математики**

**mail: *eabashkov@i.ua***

**1. Написати листа. Вказати ПІБ та групу. В  
темі завжди писати **2022CRIPTKIB19****

**2. На Github <https://github.com> и  
подключитися до репозитарію  
**eabshkvprof/2022\_Cript****

**Можна зайти**

**[https://github.com/eabshkvprof/2022\\_Cript](https://github.com/eabshkvprof/2022_Cript)**

**Команда MS Teams [2021-2021. КІБ-19.Криптозахист](#)**

# ОБЪЕМ УЧЕБНОЙ РАБОТЫ

- Всего 5 кредитов , 150 часов
- Аудиторные
  - Лекции 14 часов - 8 лекций
  - Практические 32 часа - 16 практик
- Курсовая работа
- Экзамен

# ТЕМАТИКА

## Тема 1. Вступ.

Методи захисту інформації. Криптографія. Класифікація криптографічних методів захисту інформації.

## Модульні обчислення.

Арифметика цілих чисел. Бінарні операції. Теорія подільності. НСД і алгоритм Евкліда. Рішення лінійного діафантова рівняння. Модульна арифметика. Відрахування і система відрахувань. Операції в множині відрахувань. Матриці відрахувань.

# ТЕМАТИКА

## Тема 2. Симетричні криптосистеми.

Шифри, засновані на відрахуваннях. Шифри підстановок (моноалфавітний, багатоалфавітний, роторні). Шифри перестановок. Шифри потоку. Основи блокових шифрів із симетричними ключами. Операції циклічного зсуву, заміни, розбиття, об'єднання, розсіювання, перемішування. Раунди. Шифр Файстеля, шифр не-Файстеля. Сучасні підходи до шифрів потоку. Шифри DES, AES, «Каліна». Режим роботи. Поточкові шифри RC4, «Струмок».

# ТЕМАТИКА

## Тема 3. Асиметричні криптосистеми.

*Прості числа.* Взаємно прості числа. Пошук простих чисел. Решето Ератосфена. Генерація простих чисел. Випробування простоти числа.

*Алгебраїчні структури.* Групи, підгрупи, кільця. Поля Галуа. Операції в полі Галуа: модуль, додавання, множення. Поліноми. Мультиплікативної групи, структура, знаходження зворотних елементів. Методи розкладання на множники. Китайська теорема про залишки. Квадратичне порівняння. Піднесення до степеню і логарифми. Дискретний логарифм. Функції шифрування-дешифрування RSA. Визначення ключової пари RSA. Секретні і відкриті ключі. Прокол обміну ключами Диффи-Хеллмана (DH).

# ТЕМАТИКА

## Тема 4. Хешування.

Одно направлена хеш функція. Огляд. Алгоритми хешування: сімейство SHA, сімейство MD. Хеш функції на базі блочних алгоритмів. Функція хешування «Купина».

# ОЦЕНКА

## Практические занятия.

2 практики = → 1 опрос → max 5 балл.

в сумме до 40 баллов

Экзамен 60 баллов

ИТОГО: 100 баллов

*Бонус !!! каждое посещение пары*

*→ 0, 5 балла, max 10 балл.*



# ЛИТЕРАТУРА

**Нечаев В.И.** Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.: ВШ., 1999.- 109 с.

Введение в криптографию. Под общ. ред.  
**В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012  
– 348 с. ISBN 978-5-4439-0026-1

# ЛИТЕРАТУРА

**Венбо Мао.** Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7  
(рус.)

**Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. — Москва: Вильямс, 2016. 1024 с.

# ЛИТЕРАТУРА

**Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.**

**Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.**

**A. Menezes, P. van Oorschot, S. Vanstone.**

**Handbook of Applied Cryptography.- CRC Press, 1996.**

# ИСТОРИЯ

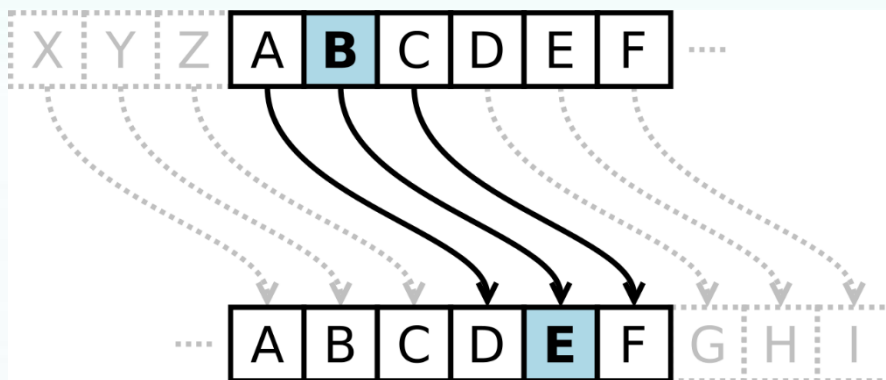
ПЕРИОД	
3 тыс. лет до НЭ	Моноалфавитные шифры
IX ВЕК НЭ	Полиалфавитные шифры
1910 → 1940	Полиалфавитные шифры + Механика / Электромеханика
1940 → 1970	Использование математики (К. Шенон), секретный ключ
1970 → .....	Криптография с открытым ключом

# ИСТОРИЯ



СКИТАЛА

Спарта, 5 век до НЭ



ШИФР ЦЕЗАРЯ

Рим, 1 век до НЭ

# ИСТОРИЯ

## Шифры монахов (XIII – XIV века)



### Цистерианская система счисления

1.993	4.723	6.859	7.085	9.433

1	2	3	4	5	6	7	8	9
10	20	30	40	50	60	70	80	90
100	200	300	400	500	600	700	800	900
1.000	2.000	3.000	4.000	5.000	6.000	7.000	8.000	9.000

# ИСТОРИЯ



**Фрэнсис Бэкон (1580) ! двоичный способ кодирования латинского алфавита**

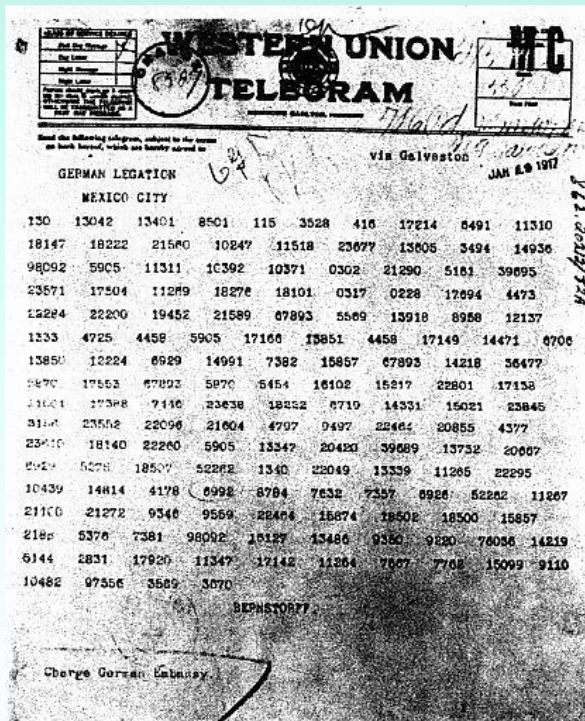
**Блез де Виженер  
1585 - !!! Ключ**





# ИСТОРИЯ

## Кодированная телеграмма министра иностранных дел Германии (1916)



«Энигма», патент от 1917  
(Хьюго Кох, Голландия)



# ИСТОРИЯ

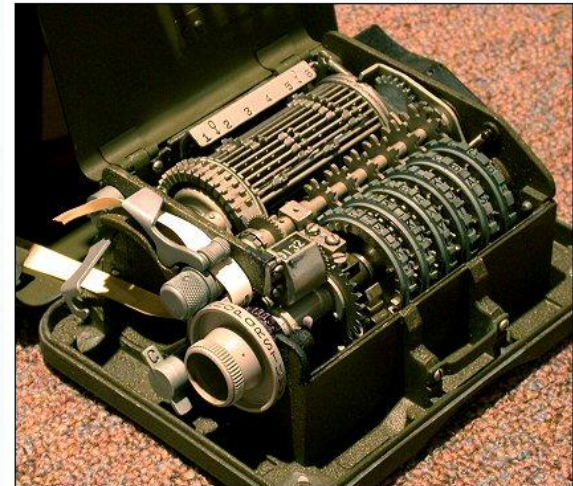


Машина Лоренца  
Lorenz SZ 40, "Fish"  
(Германия, 1940)

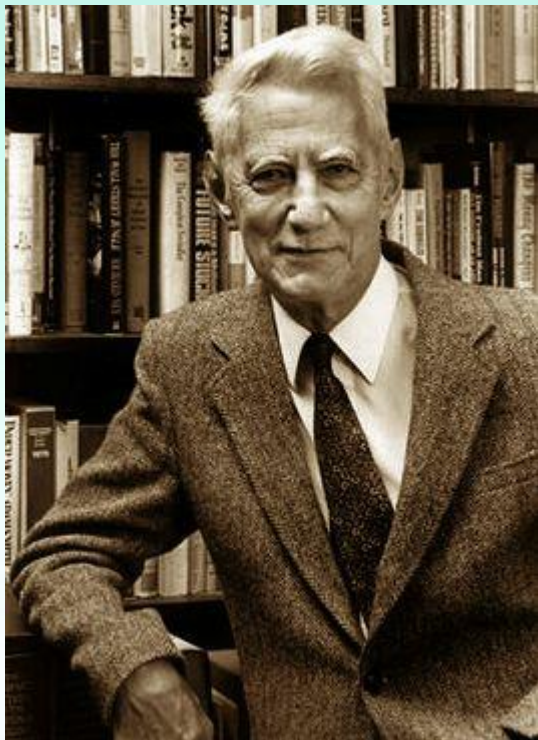
Машина М-209  
(США, 1940)



HAGELIN M-209 CIPHER MACHINE (GVG / PD)



# ИСТОРИЯ



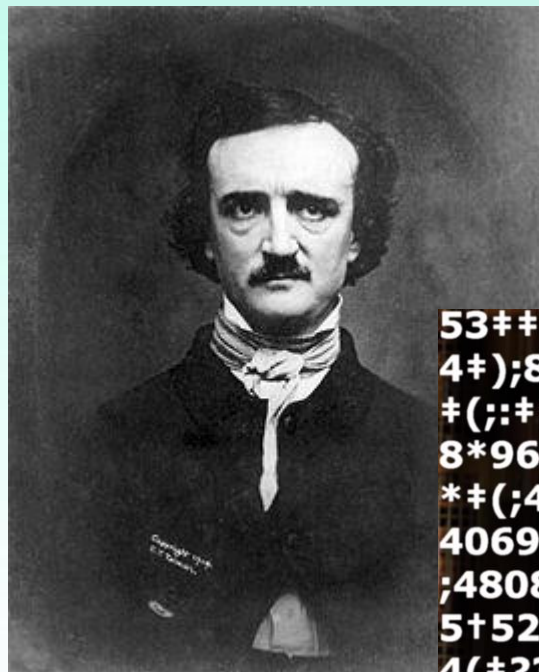
Клод Шенон,  
«Теория связи в секретных  
системах» (США, 1945) :

*Математизация*

Уитфилд Диффи, Мартин Хеллман  
«Новые направления в криптографии»,  
(США, 1976): *Открытый ключ*



# Криптография в литературе

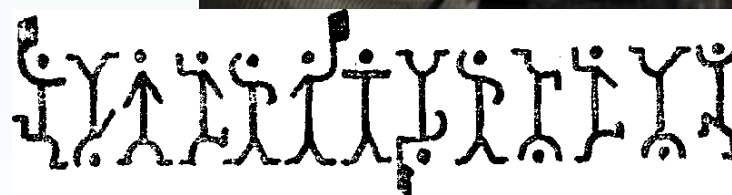


Эдгар Аллан По,  
«Золотой жук» (США, 1843)

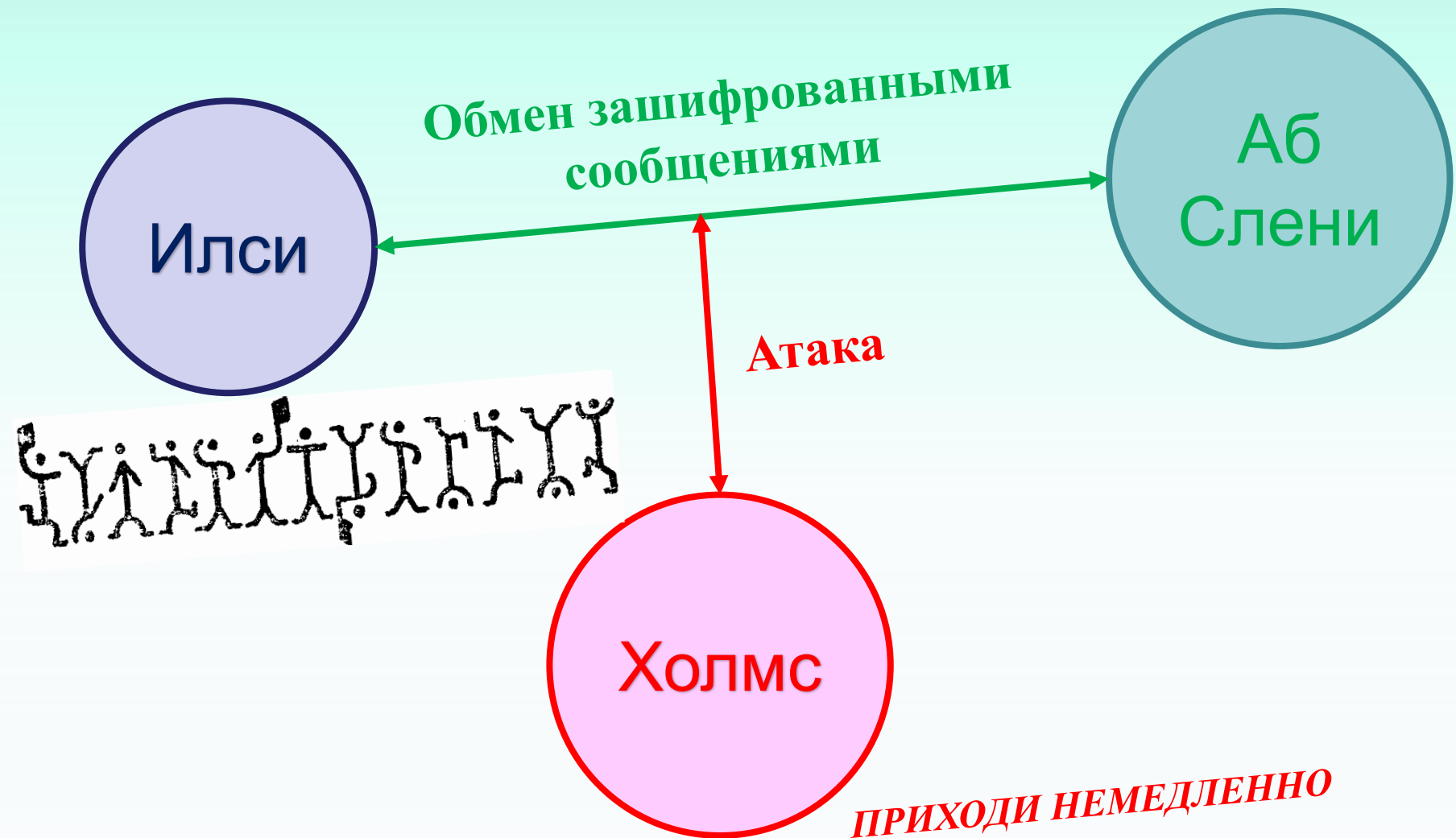
53##†305))6\*;4826)4#.)  
4#);806\*;48†8¶60))85;1  
#(;;#\*8†83(88)5\*†;46(;8  
8\*96\*?;8)\*#(;485);5\*†2:  
\*#(;4956\*2(5\*—4)8¶8\*;  
4069285);)6†8)4##;1(†9  
;48081;8:8†1;48†85;4)48  
5†528806\*81(†9;48;(88;  
4(†?34;48)4#;161;;188;#?;



Артур Конан Дойль  
«Пляшущие человечки»  
(Великобритания, 1905)

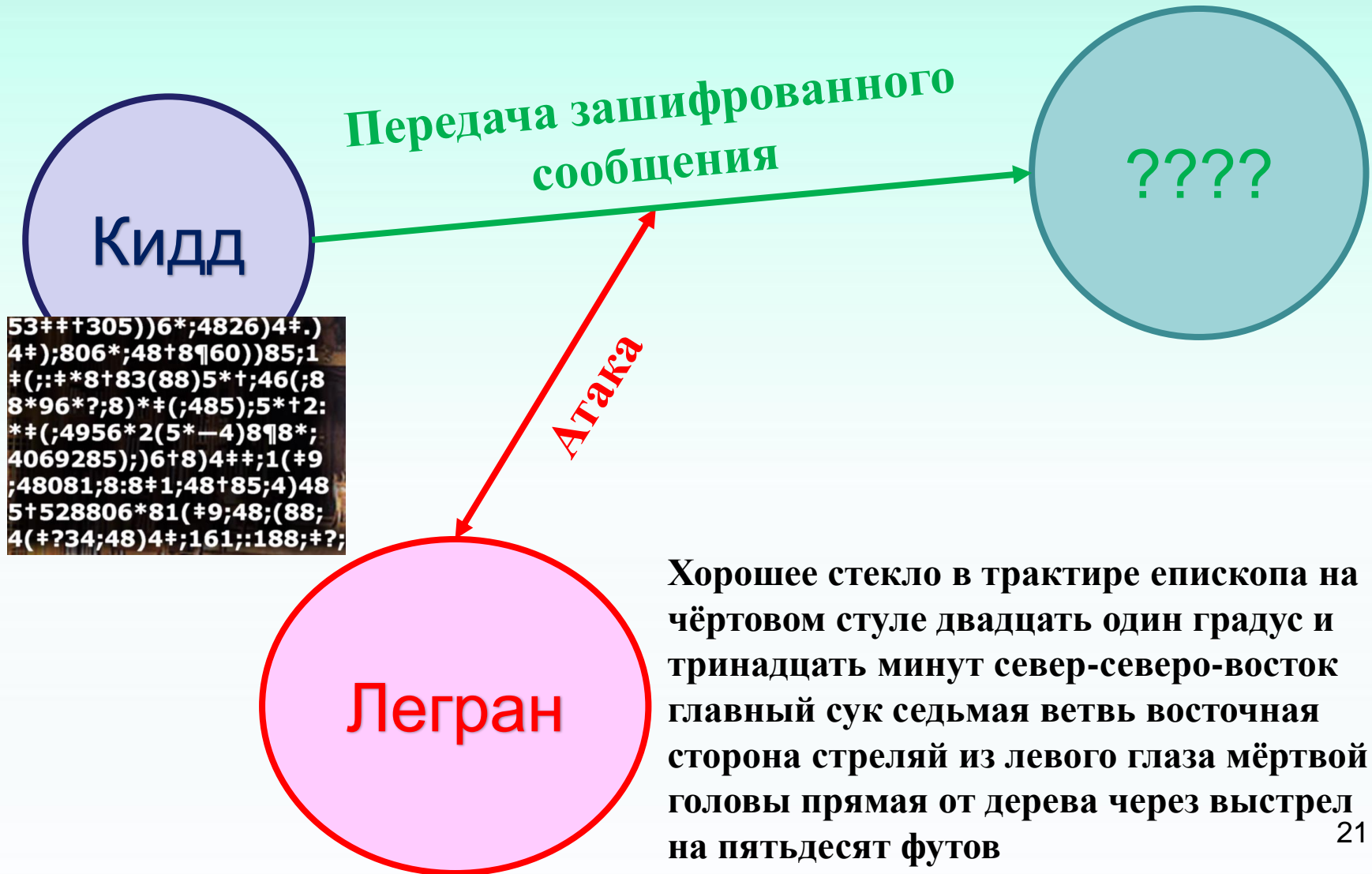


# Резюме 1. Артур Конан Дойль





# Резюме 2. Э.А. По

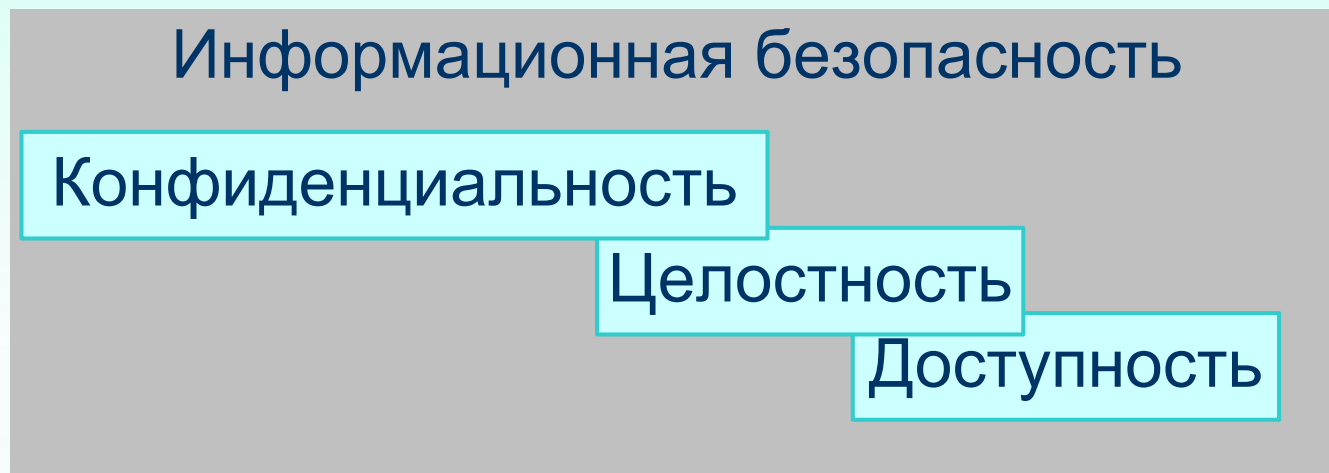


# ВЫВОД



# Информационная безопасность

**Информационная безопасность** — состояние сохранности информационных ресурсов и защищенности законных прав личности и общества в информационной сфере.



**Информационная безопасность** — это процесс обеспечения конфиденциальности, целостности и доступности информации.

# Информационная безопасность

## Конфиденциальность

**Конфиденциальность** — обеспечение доступа только авторизованным (правильным) пользователям.

*!!! Важно обеспечение конфиденциальности информации как при ее **хранении**, так и при ее **передаче***



# Информационная безопасность

## Целостность

**Целостность** — обеспечение достоверности и полноты информации и методов ее обработки.

*!!! Изменение информации возможно только «правильными» объектами (пользователями, программами, ....).*

# Информационная безопасность

## Доступность

**Доступность** — обеспечение доступа к информации и связанным с ней активам исключительно авторизованным пользователям и только по мере необходимости.

*!!! Информация бесполезна, если она не доступна.*

# Угрозы : Атаки

## Угрозы конфиденциальности

**Вмешательство**

**Анализ трафика**

**Вмешательство** –  
неправомерный доступ и / или перехват данных.

**Анализ трафика** –  
извлечение информации из трафика (адреса, активность, ....).

# Угрозы : Атаки

## Угрозы целостности

Модификация

Имитация

Отказ

Повтор

**Модификация** – атакующий изменяет передаваемую информацию.

**Имитация** – атакующий имитирует «правильный» источник/приемник.

**Отказ** – отрицание факта приема/передачи информации.

**Повтор** – повторная передач от атакующего.

# Угрозы : Атаки

## Угрозы доступности

### Отказ обслуживания

**Отказ в обслуживании (Denial of Service — DoS) —**

постоянное или временное прерывание обслуживания в запросах на информацию.

**Пассивные атаки** — цель атакующего только в получении информации (атаки на конфиденциальность)

**Активные атаки** — цель атакующего в изменении данных и / или повреждение системы (атаки на целостность, доступность)

# Угрозы злоумышленника (Eve)

**Злоумышленник (противник, перехватчик, взломщик, intruder) – субъект, который пытается нарушить безопасность системы (атакует систему).**

- 1. Ознакомление с содержанием переданного сообщения.**
- 2. Навязывание** получателю **ложного** сообщения – **полная фабрикация** и/или **внесение искажений**
- 3. Изъятие** переданного сообщения, дабы **получатель** и не **знал** о факте передачи
- 4. Нарушение работоспособности канала связи**

# Угрозы законного отправителя (Alice)

1. **Разглашение** переданного сообщения
2. **Отказ** от авторства в действительности переданного им сообщения
3. **Утверждение**, что некоторое сообщение было отправлено получателю, когда в действительности отправка не производилась.

# Угрозы законного получателя (Bob)

1. **Разглашение** переданного сообщения
2. **Отказ** от факта получения некоторого сообщения, когда в действительности оно им было получено.
3. **Утверждение**, что некоторое сообщение получено от отправителя, когда в действительности предъявленное сообщение сфабриковано самим получателем .



# Криптография

Наука **Криптогра́фия** от др. греческого **криπτός** «скрытый» + **γράφω** «пишу» —

наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

# Основной метод криптографии

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

Шифрование обеспечивает:

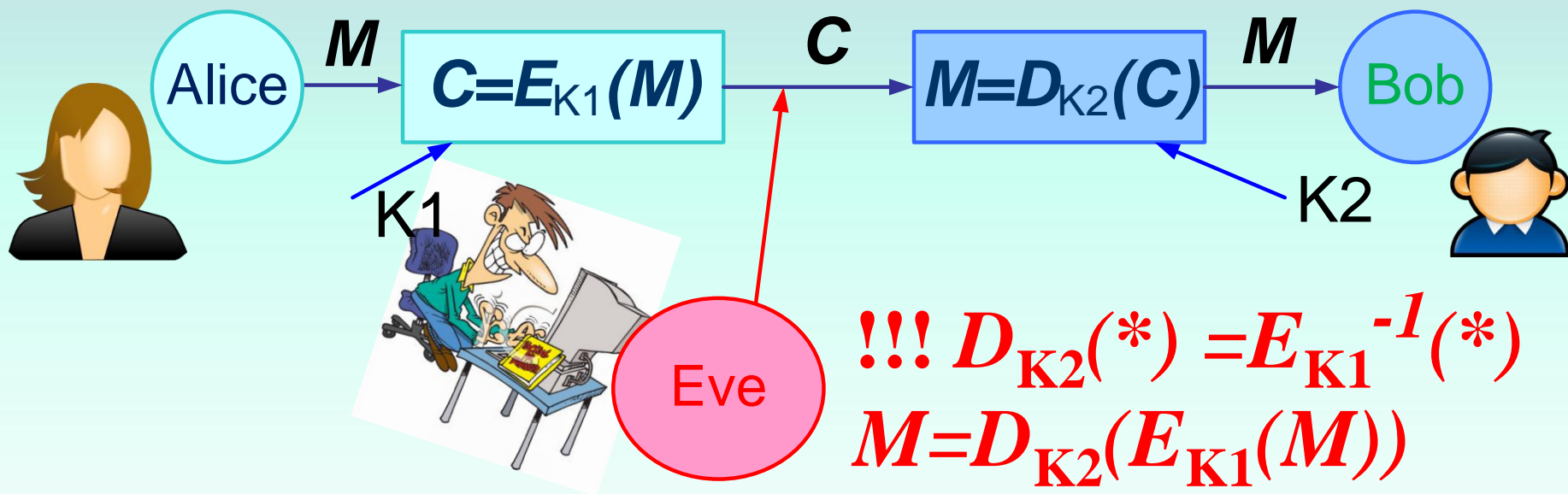
- ***Конфиденциальность*** — сокрытие информации от неавторизованных пользователей;
- ***Целостность*** — предотвращение изменения информации при передаче и хранении;
- ***Идентифицируемость*** — предотвращение отказов.

# ШИФР

**ШИФР** — от фр. **chiffre** «цифра» + араб. **صِفْر**, **sifr** «ноль») —

**система обратимых преобразований (функций), зависящая от некоторого секретного параметра (ключа) и предназначенная для обеспечения секретности передаваемой информации.**

# Шифрование



$M$  – *message, plaintext* - открытый текст

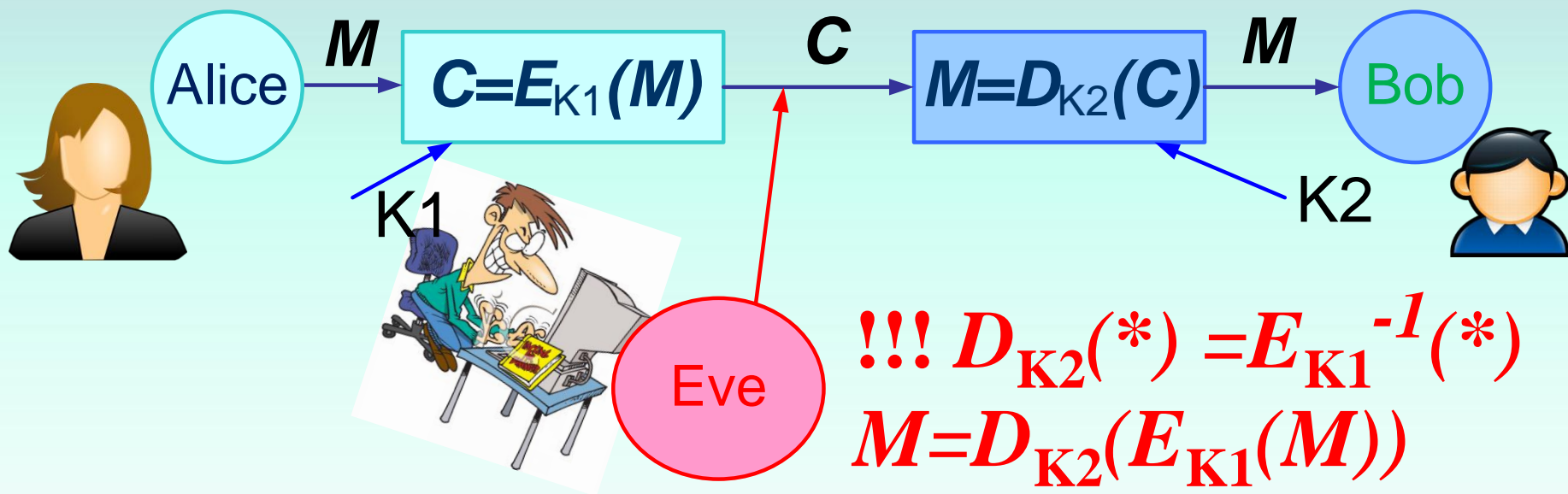
$C$  – *ciphertext* - шифротекст

$E: M \xrightarrow{k1} C$  – *encoder, encipher* – функция шифрования

$D: C \xrightarrow{k1} M$  – *decoder, decipher* – функция  
дешифрования

$k1, k2$  – *key* – ключи шифрования и дешифрования

# Алгоритм шифрования



**Cipher (сайфер)** – криптографический алгоритм шифрования (шифр) – математическая функция, которая используется для шифрования / дешифрования.

# ФУНКЦИЯ

## Функция, отображение, трансформация

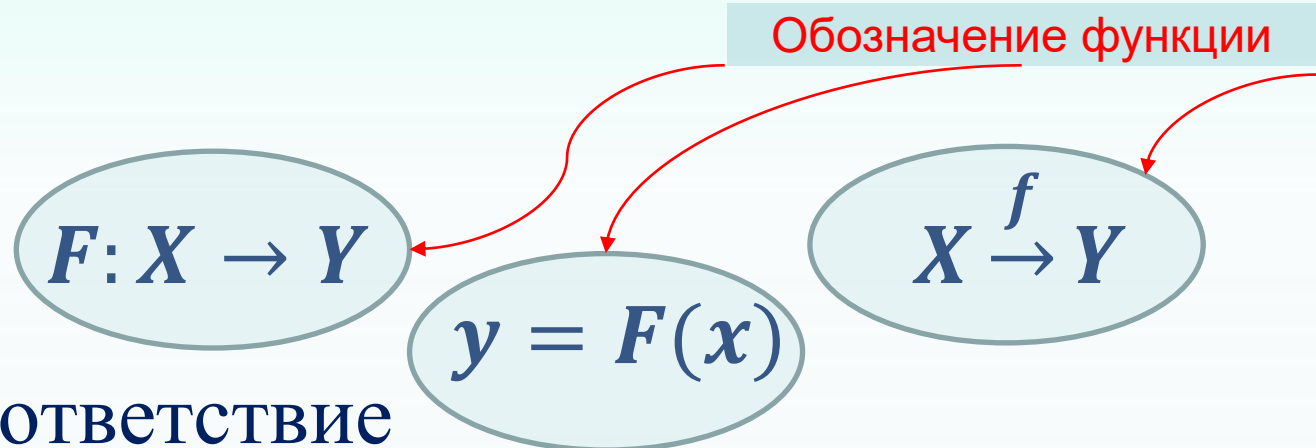
Есть некоторые множества:

$$X = \{x_1, x_2, x_3, \dots\}$$

$$Y = \{y_1, y_2, y_3, y_4, \dots\}$$

Здесь  $x_1, x_2, x_3, \dots$  ,  $y_1, y_2, y_3, y_4, \dots$  есть  
ЭЛЕМЕНТЫ МНОЖЕСТВ.

## Функция



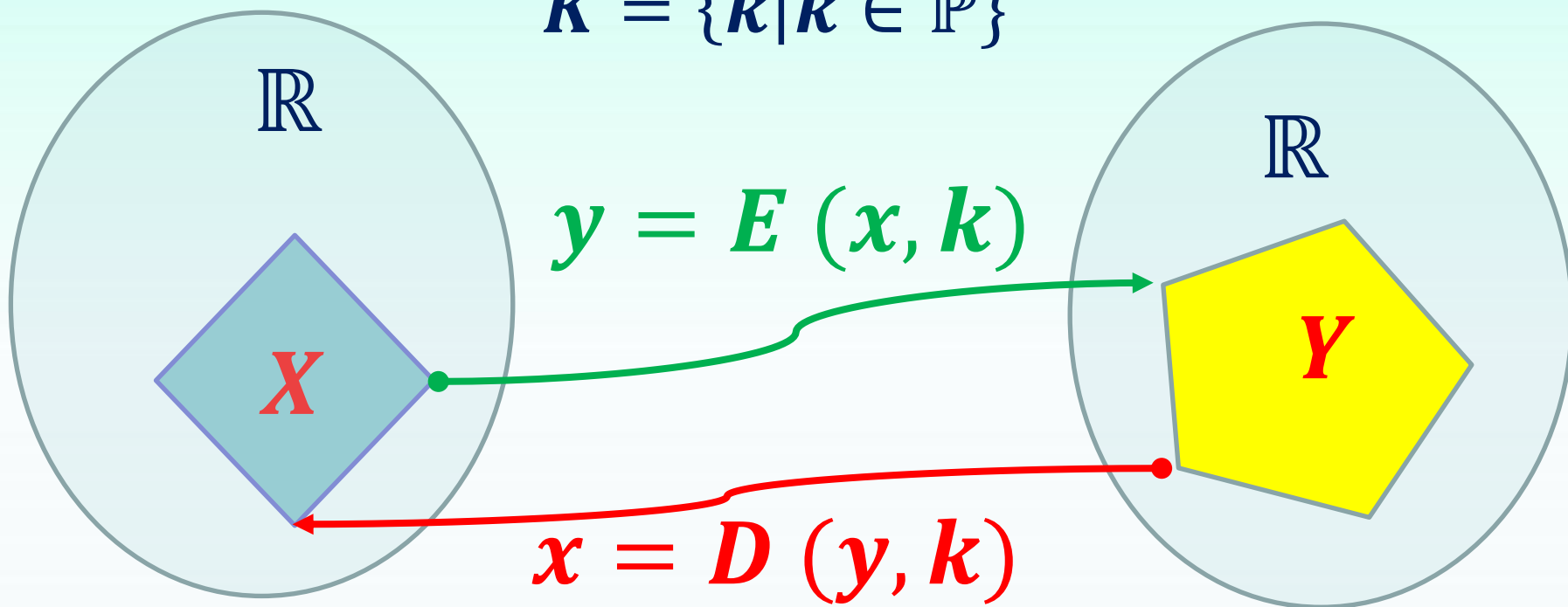
ставит в соответствие  
некоторому элементу из множества  $X$   
некоторый элемент из множества  $Y$ .

# ФУНКЦИЯ

## Функция, отображение, трансформация

$$X = \{x | x \in \mathbb{R}\}, \quad Y = \{y | y \in \mathbb{R}\}$$

$$K = \{k | k \in \mathbb{P}\}$$



? НАЙТИ  $x = D(y, k) = D(E(x, k), k)$

# Классификация

## АЛГОРИТМЫ ШИФРОВАНИЯ

СИММЕТРИЧНЫЕ  
(ОДНОКЛЮЧЕВЫЕ)

АСИММЕТРИЧНЫЕ  
(ДВУХКЛЮЧЕВЫЕ)

$$K2 = K1 = K$$

$$K2 \neq K1$$

**Симметричные** - ключ шифрования (!!секретный) может быть рассчитан по ключу дешифрования (и наоборот). В большинстве случаев – это один и тот же ключ.

**Асимметричные (с открытым ключом)** –

- ключ шифрования (открытый) - может быть опубликован;
- ключ дешифрования (закрытый) – не может быть рассчитан в «разумное» время.



# Классификация

## АЛГОРИТМЫ ШИФРОВАНИЯ

### БЛОЧНЫЕ

### ПОТОЧНЫЕ

**Блочные (block cipher)** - шифрует сразу целый блок текста, выдавая шифротекст после получения всей информации.

**Поточные (stream cipher)** - шифрует информацию и выдает шифротекст по мере поступления. Обеспечивает обработку текста неограниченного размера, используя фиксированный объем памяти

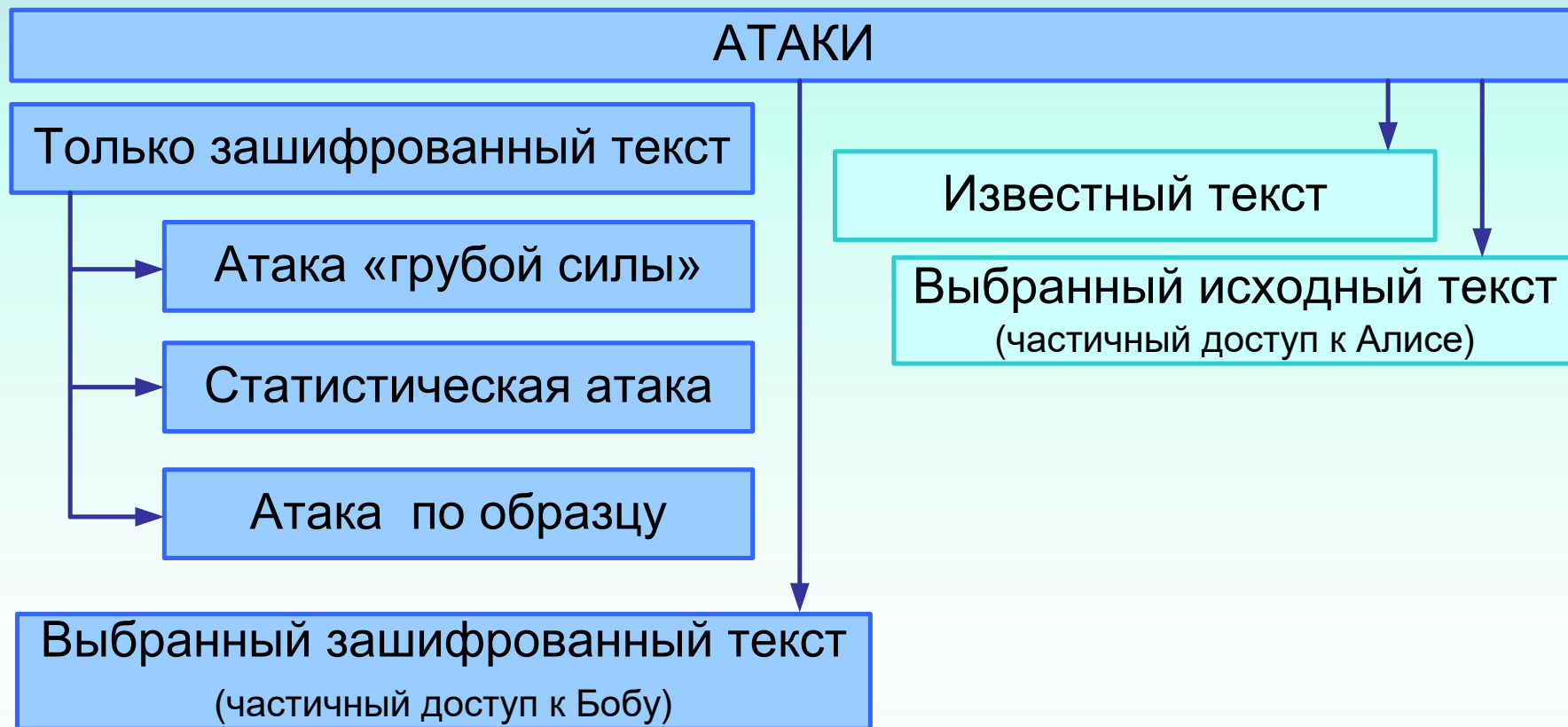
# Криптоанализ

Наука **Криптоанализ** от др. греческого **κρυπτός** «скрытый» + «анализ» — наука о методах дешифровки зашифрованной информации без предназначенного для этого ключа, а также сам процесс такой дешифровки.

**Криптоанализ** включает также методы выявления уязвимости криптографических алгоритмов или протоколов.

Попытка раскрытия шифра с применением методов криптоанализа → **криптографическая атака** на этот шифр

# Криптографическая Атака



# Криптология

Наука **Криптология** от др. греческого **κρυπτός** «скрытый» + **λόγος** «слово» —

наука, занимающаяся методами шифрования и расшифровывания

Криптология состоит из двух частей — криптографии и криптоанализа.

Криптография занимается разработкой методов шифрования данных, в то время как криптоанализ занимается оценкой сильных и слабых сторон методов шифрования, а также разработкой методов, позволяющих взламывать **криптосистемы**.<sup>44</sup>

# Вопросы:

1. Надайте основні етапи розвитку криптографії
2. Охарактеризуйте учасників обміну зашифрованими повідомленнями та їх ролі.

**Література:** Гайоронський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем — Київ: Видавнича група ВНУ, 2009. — 610 с.

# Вопросы:

- Определить ТРИ цели информационной безопасности.
- Укажите виды атак на секретную информацию.
- Дайте определение понятий: КРИПТОГРАФИЯ, КРИПТОАНАЛИЗ, КРИТОЛОГИЯ.
- Опишите механизм ШИФРОВАНИЯ.
- Какие классы алгоритмов шифрования вы знаете?
- Определите ШИФР с симметричным ключом.
- Определите ШИФР с асимметричным ключом.
- Поясните разницу между блочным и потоковым шифрами.
- Какие виды атак на шифр Вы можете описать?

# ЛИТЕРАТУРА

**Нечаев В.И.** Элементы криптографии (Основы теории защиты информации).- Учеб. пособие. – М.: ВШ., 1999.- 109 с.

**Введение в криптографию. Под общ. ред. В.В.Ященко.** – 4-е изд., доп. М.: МЦНМО, 2012 – 348 с. ISBN 978-5-4439-0026-1

# ЛИТЕРАТУРА

**Венбо Мао.** Современная криптография: теория и практика.—М.: Издательский дом «Вильямс», 2005.—768 с.: ил. ISSN 5-8459-0847-7  
(рус.)

**Шнайер Б.** Прикладная криптография. Протоколы, алгоритмы и исходный код на Си. — Москва: Вильямс, 2016. 1024 с.



# ЛИТЕРАТУРА

**Francisco Rodriguez-Henriquez, N.A. Saqib, A. Diaz-Perez, Cetin Kaya Koc.**

**Cryptographic Algorithms on Reconfigurable Hardware. - Springer, 2006.**

**A. Menezes, P. van Oorschot, S. Vanstone.**

**Handbook of Applied Cryptography.- CRC Press, 1996.**

**END # 1**