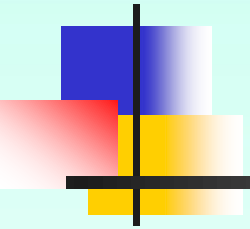


CRYPTOGRAPHY

МАТЕМАТИЧНІ МЕТОДИ КРИПТОГРАФІЇ

Лек. 1 2022 КІБ-20

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 2022CRYPT20

2. На Github https://github.com підключитися до репозитарію eabshkvprof/2022_Math_Crypt

Можна зайти
https://github.com/eabshkvprof/2022_Math_Crypt

Команда MS Teams 2022-2023. КІБ-20.Math_Crypt

ОБЪЕМ УЧЕБНОЙ РАБОТЫ

- **Всего** 6 кредитов , 180 часов
- **Аудиторные**
  - Лекции 32 часа - 16 лекций
  - Практические 32 часа - 16 практик
- **Расчетная Работа**
- **Экзамен**

ТЕМАТИКА

Тема 1. Вступ.

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

Тема 2. 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. Шифри, засновані на відрахуваннях. Шифри підстановок (моноалфавітний, багатоалфавітний, роторні). Шифри перестановок. Шифри потоку. Блокові шифри.

ТЕМАТИКА

Тема 3. Алгебраїчні структури.

Групи, підгрупи. Кільця. Алгебраїчні структури. Поля. Поля Галуа (GF (pn)). Операції в полі GF(2n): модуль, додавання, множення. Поліноми в GF(2), GF (2n).

Основи блокових шифрів із симетричними ключами. Операції циклічного зсуву, заміни, розбиття, об'єднання, розсіювання, перемішування. Раунди. Шифр Файстеля, шифр не-Файстеля.

Стандарти DES, AES, «Каліна». Режими роботи. Сучасні підходи до шифрів потоку. Потокові шифри RC4, «Струмок».

ТЕМАТИКА

Тема 4. Прости числа.

Взаємно прості числа. Пошук простих

чисел. Решето Ератосфена. Генерація простих чисел. Випробування простоти числа.

Побудова мультиплікативної групи кільця по модулю N = PQ, визначення порядку мультиплікативної групи кільця и максимального порядку елементів мультиплікативної групи. Структура мультиплікативної групи кільця. Phi-функція Ейлера. Теорема Ейлера. Знаходження зворотних елементів мультиплікативної групи.

ТЕМАТИКА

Тема 5. Множники.

Методи розкладання на множники (Ферма, Полларда). Китайська теорема про залишки. Квадратичне порівняння. Піднесення до степеня і логарифми. Дискретний логарифм. Асиметричні криптосистеми на базі кілець. Функції шифрування-дешифрування RSA. Секретні и відкриті ключі. Визначення ключової пари RSA.

Тема 6. Еліптичні криві.

Абелєва група і додавання точок на еліптичній кривій. Еліптичні криві в GF(p). Еліптичні криві в GF(2n). Використання еліптичних кривих в криптографії.

ТЕМАТИКА

Розрахункова Робота. Хешування.

Розробити програмний засіб обчислення хеш дайджесту відкритого повідомлення. Реалізація індивідуального завдання передбачає залучення можливостей стандартної Python бібліотеці HashLib та написання власного програмного скрипту.

ОЦЕНКА

Практические занятия.

2 практики = → 1 опрос → мах 5 балл.

в сумме до 40 баллов

Экзамен 60 баллов

ИТОГО: 100 баллов

Бонус !!! каждое посещение пары

→ 0, 5 балла, мах 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.

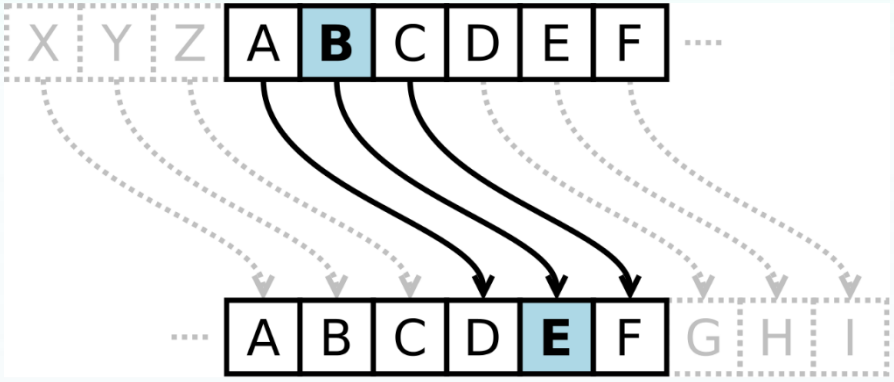
Handbook of Applied Cryptography.- CRC Press, 1996.

ИСТОРИЯ

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

ИСТОРИЯ

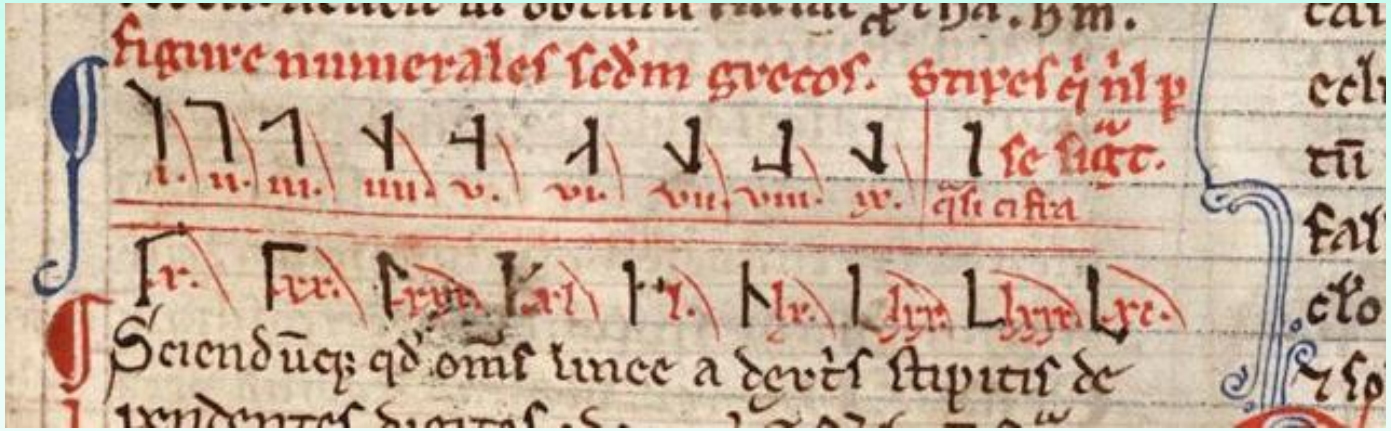
СКИТАЛА
Спарта, 5 век до НЭ



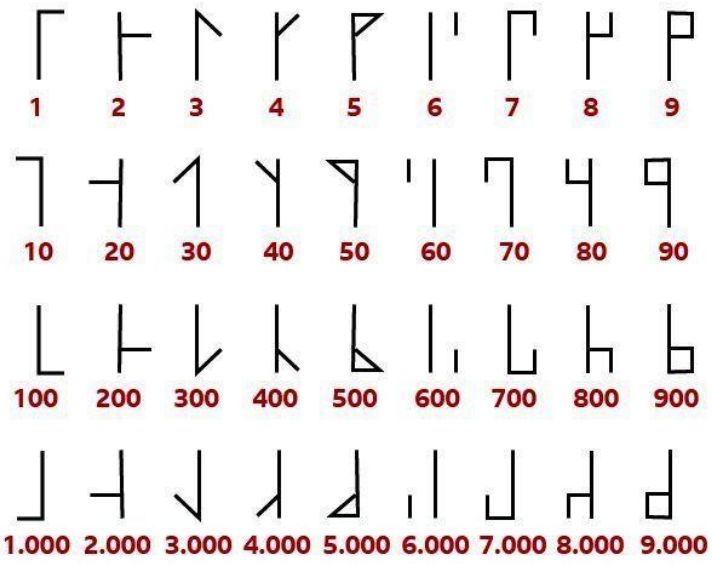
ШИФР ЦЕЗАРЯ
Рим, 1 век до НЭ

ИСТОРИЯ

Шифры монахов (XIII – XIV века)



Цистерианская система счисления

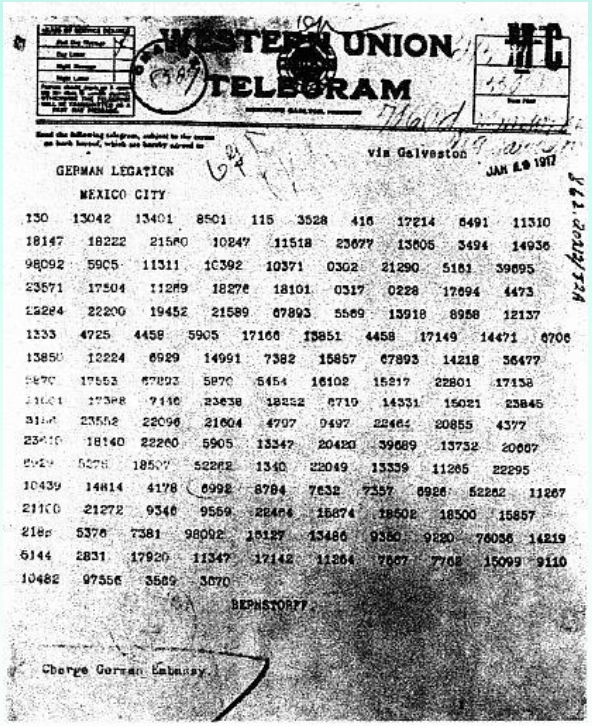


ИСТОРИЯ

Фрэнсис Бэкон (1580) ! двоичный способ кодирования латинского алфавита

Блез де Виженер
1585 - !!! Ключ

ИСТОРИЯ



WESTERN UNION TELEGRAM

via Galveston

JAN 19 1917

GERMAN LEGATION
MEXICO CITY

130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22224 22200 19452 21589 67893 5569 13918 8958 12137
1233 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
9870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7110 23638 18252 6719 14331 15021 23845
31[illegible] 23552 22096 21604 4797 9497 22464 20855 4377
23[illegible] 18140 22260 5905 13342 20420 39689 13732 20667
9[illegible] 5[illegible] 18[illegible] 52282 1340 22049 13339 11265 22295
10439 14814 4178 6992 8784 7632 7357 6926 52282 11267
21100 21272 9346 9559 22464 15874 18502 18500 15857
218[illegible] 5376 7381 98092 16127 13486 9350 9220 76036 14219
6144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

ZIMMERMANN

Charge German Embassy.

Кодированная телеграмма министра иностранных дел Германии (1916)

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

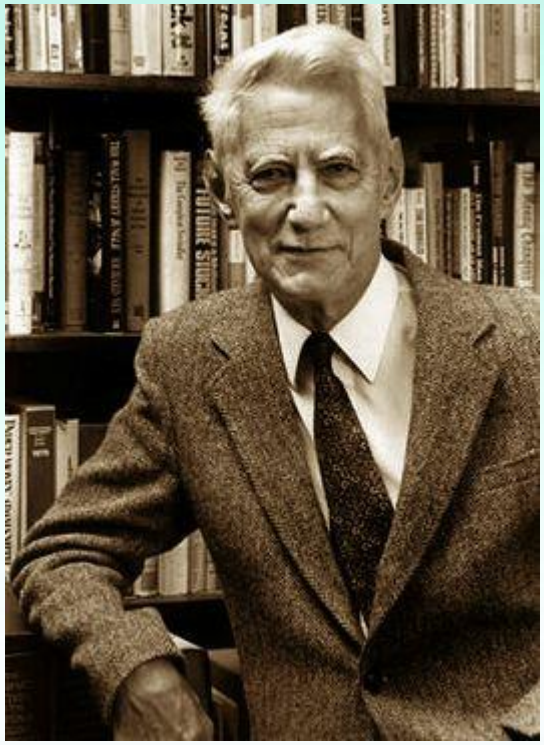
ИСТОРИЯ

Машина Лоренца
Lorenz SZ 40, “Fish”
(Германия, 1940)

HAGELIN M-209 CIPHER MACHINE (GVG / PD)

Машина М-209
(США, 1940)

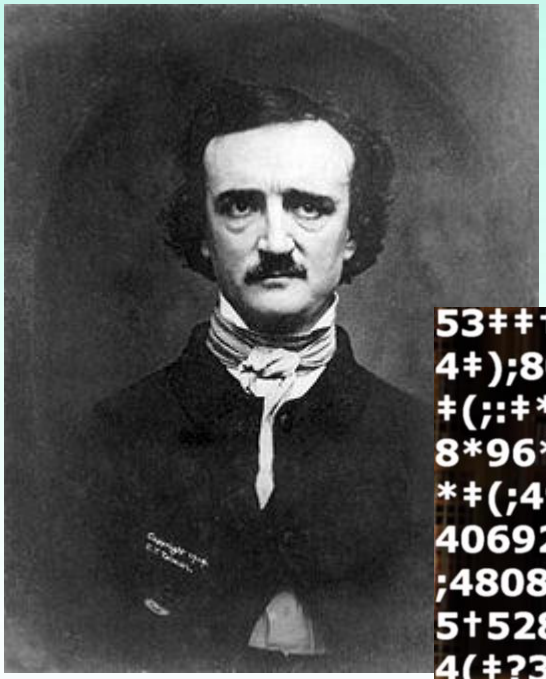
ИСТОРИЯ



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

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

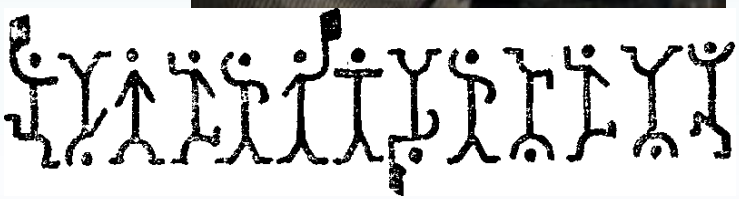
Криптография в литературе



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

Обмен зашифрованными сообщениями

Илси

Аб Слени

Атака

Холмс

ПРИХОДИ НЕМЕДЛЕННО

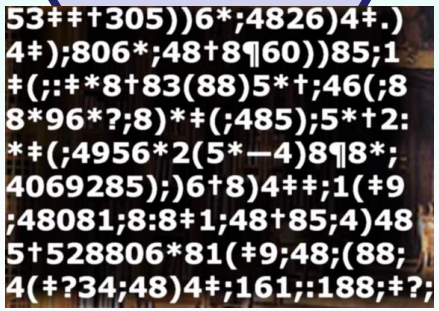
Резюме 2. Э.А. По

Передача зашифрованного сообщения

Кидд

????

Атака



Легран

Хорошее стекло в трактире епископа на чёртовом стуле двадцать один градус и тринадцать минут север-северо-восток главный сук седьмая ветвь восточная сторона стреляй из левого глаза мёртвой головы прямая от дерева через выстрел на пятьдесят футов

ВЫВОД

Alice

Передача зашифрованного сообщения

Bob

Alice / Алиса
Отправитель

Атака

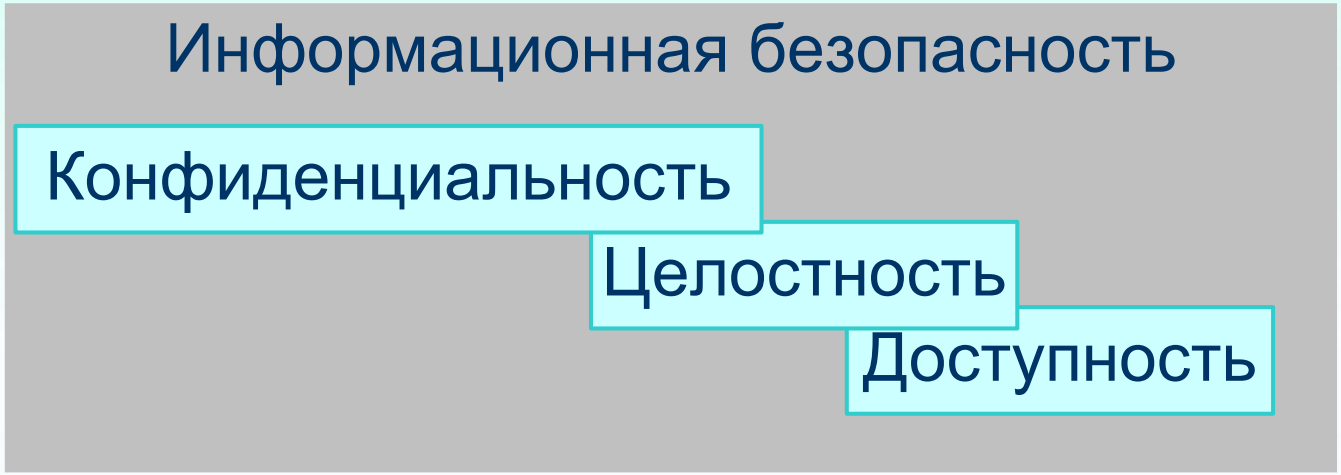
Bob / Боб
Получатель

Eve / Mallory

Eve / Ева : Перехватчик
Mallory / Мэлори : Злонамеренный активный взломщик

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 κρυπτός «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:

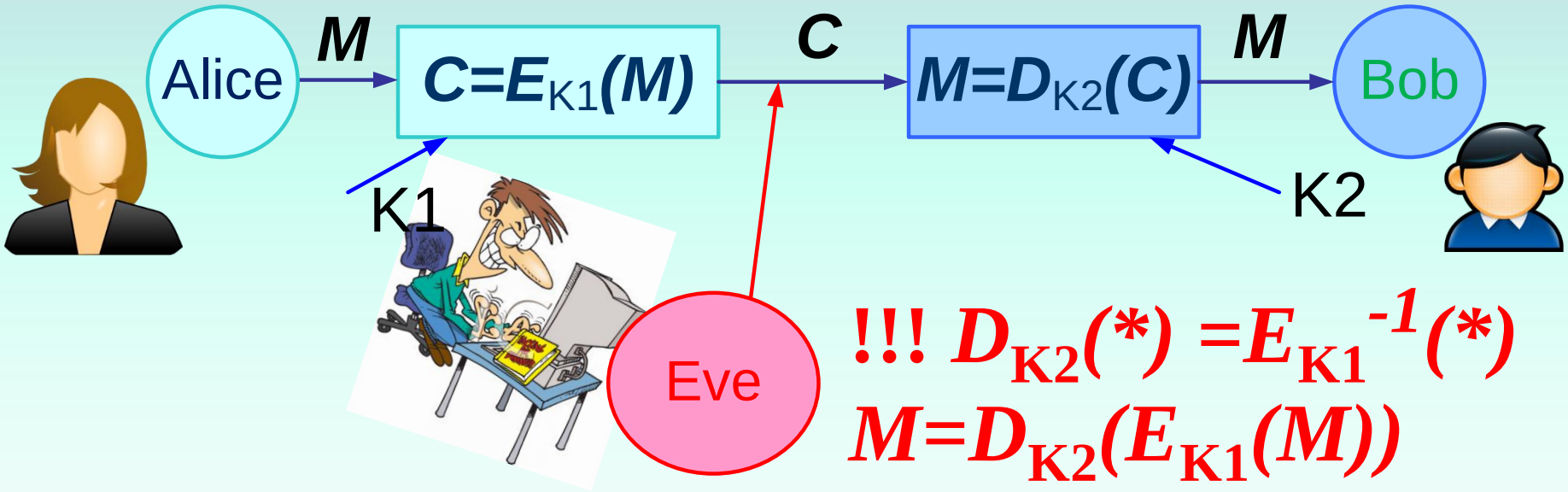
- ***Конфиденциальность*** – сокрытие информации от неавторизованных пользователей;
- ***Целостность*** – предотвращение изменения информации при передаче и хранении;
- ***Идентифицируемость*** – предотвращение отказов.

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



$!!!\ D_{K2}(*) = E_{K1}^{-1}(*)$

$M = D_{K2}(E_{K1}(M))$

M – *message, planetext* - открытый текст

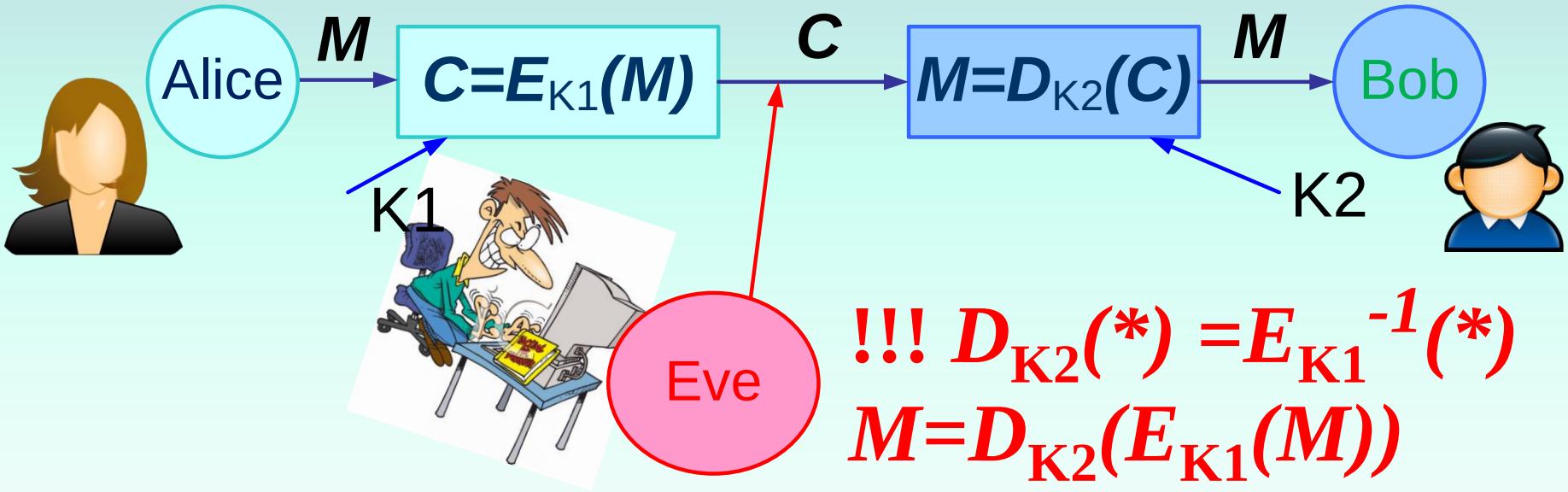
C – *ciphertext* - шифротекст

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

$\boldsymbol{D}: \boldsymbol{C} \underset{k2}{\rightarrow} \boldsymbol{M}$ – *decoder, decipher* – функция дешифрования

k1, k2 – key – ключи шифрования и дешифрования

Алгоритм шифрования



$$!!!\ D_{K2}(*) = E_{K1}^{-1}(*)$$

$$M = D_{K2}(E_{K1}(M))$$

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

ФУНКЦИЯ

Функция, отображение, трансформация

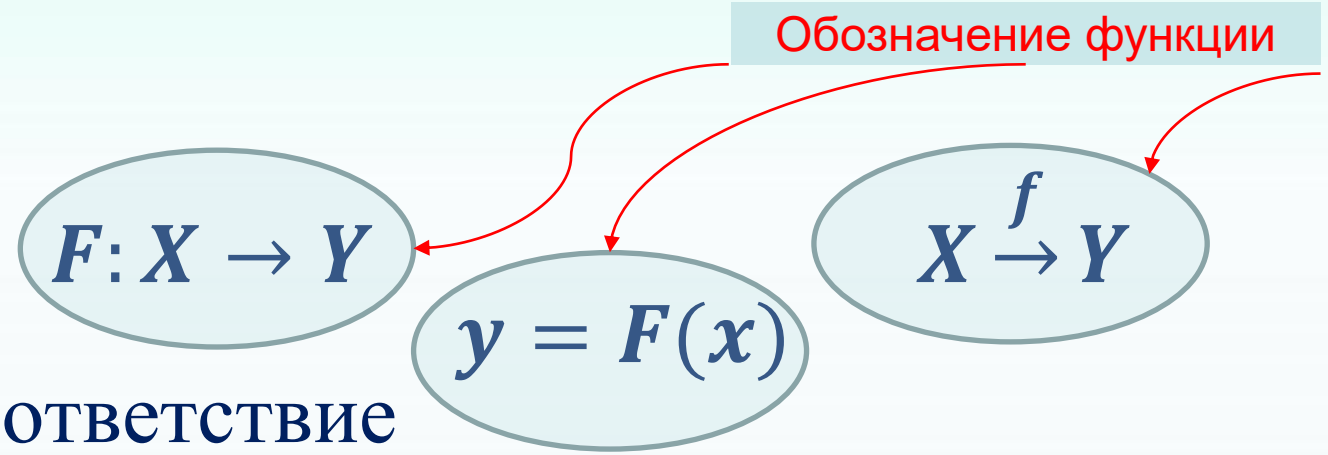
Есть некоторые множества:

$$X = \{x1, x2, x3, \dots\}$$

$$Y = \{y1, y2, y3, y4, \dots\}$$

Здесь $x1, x2, x3, \dots$, $y1, y2, y3, y4, \dots$ суть элементы множеств.

Функция



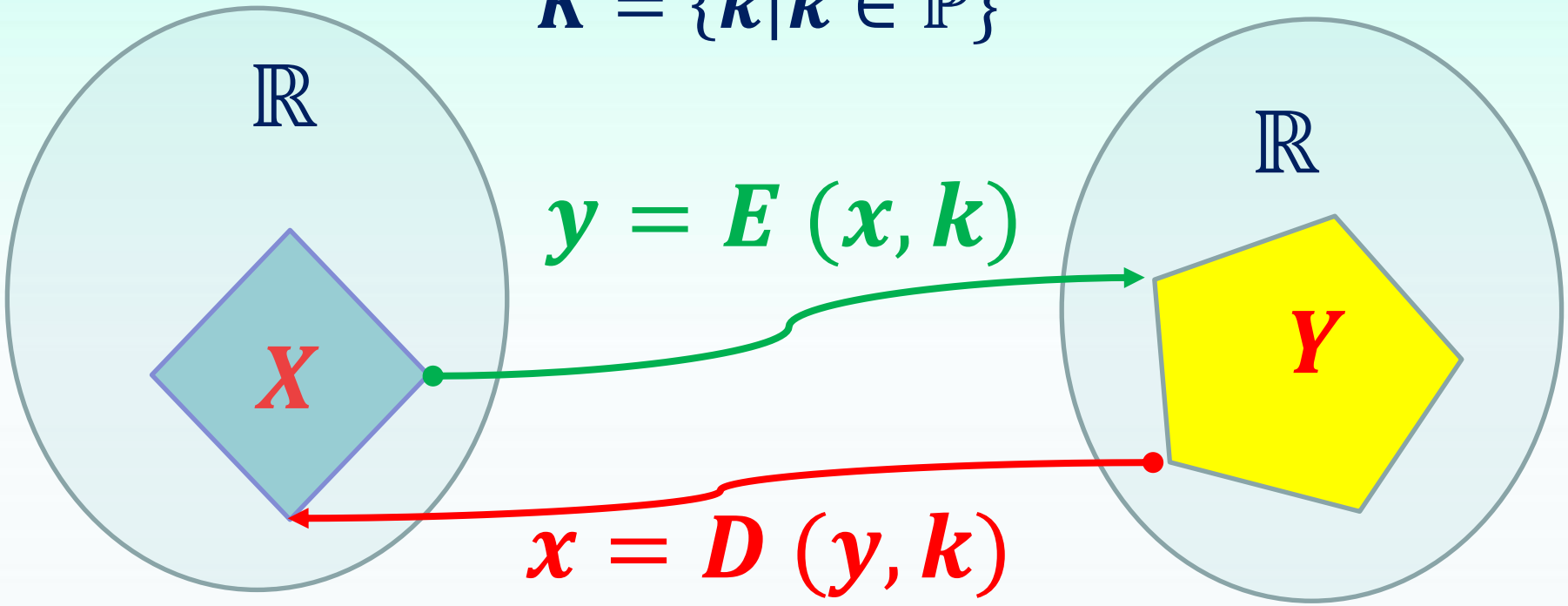
ставит в соответствие некоторому элементу из множества X некоторый элемент из множества Y .

ФУНКЦИЯ

Функция, отображение, трансформация

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

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



? НАЙТИ $x = D(y, k) = D(E(x, k), k)$

Классификация

АЛГОРИТМЫ ШИФРОВАНИЯ

СИММЕТРИЧНЫЕ (ОДНОКЛЮЧЕВЫЕ)	АСИММЕТРИЧНЫЕ (ДВУХКЛЮЧЕВЫЕ)
K2 = K1= K	**K2 ≠ 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

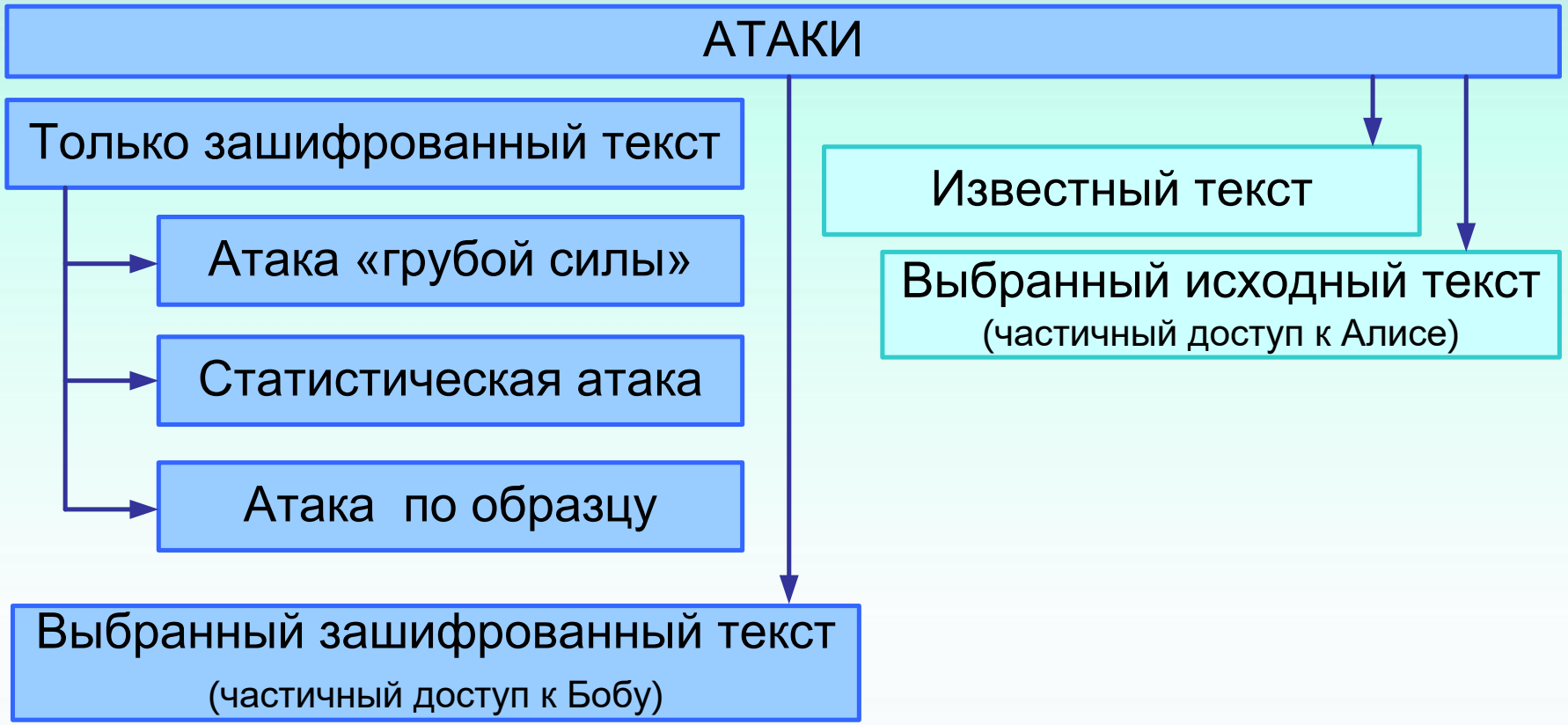
Криптоанализ

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.**

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 BHV, 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