

# Методы шифрования.

Выполнила Круглова  
Ангелина.

# Шифрование.

- ✓ Шифрование данных - это методы защиты любой информации от несанкционированного доступа, просмотра, а также её использования, основанные на преобразовании данных в зашифрованный формат.

Расшифровать, восстановить данную информацию или сообщение, обычно можно только при помощи ключа, который применялся при его зашифровании.

Шифрование состоит из двух взаимобратимых процессов - зашифровывания и расшифровывания.

- ✓ Криптология — наука, занимающаяся методами шифрования и дешифрования. 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.

# Методы шифрования.

## ✓ Симметричное шифрование

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ. Отсюда название — симметричные. Алгоритм и ключ выбирается заранее и известен обеим сторонам. Сохранение ключа в секретности является важной задачей для установления и поддержки защищённого канала связи.



## ✓ Алгоритмы симметричного шифрования.

- Поточковые шифры - это шифры, при которых каждый бит информации шифруется с помощью наложения на открытые данные гаммы шифра по определенному правилу. Для расшифрования та же гамма накладывается на зашифрованный текст.
- Чаще других используются блочные шифры. Информация, которую хотят зашифровать делится на блоки определенной длины, и шифруется поблочно.

○



A7CE203	G0030200	01208600	37D14D00
B7125G0	024FG002	53D03C00	AD722500
BD03C00	887525C1	01A07700	37D14D00
37125G0	024FG002	53D03C00	AD722500
D03C00	887525C1	4F553F	5341424
4F3D41	4242434E	3D4A6	2 6469204
5C2F4F	553D4553	414	3 4F3D41
125604	00312E30	424	31 000342
03042	4CC	6 024E4E4F	00B1D3
254F1	21	309 8833B0CC	2957E
3ECAA	CB3EE8EF	DF038D7F	A1421
AA4D	04143B75	4F571C83	535C0
DED9	B57C659E	C820EE07	FA49E
96DB	7D7F743D	9A36DD29	454E

## ✓ Асимметричное шифрование

В системах с открытым ключом используются два ключа — открытый и закрытый. Открытый ключ передаётся по открытому (то есть незащищённому, доступному для наблюдения) каналу и используется для шифрования сообщения. Для расшифровки сообщения используется секретный ключ.

Данная схема решает проблему симметричных схем. Если в симметричных схемах злоумышленник перехватит ключ, то он сможет как «слушать», так и вносить правки в передаваемую информацию. В асимметричных системах другой стороне передается открытый ключ, который позволяет шифровать, но не расшифровывать информацию.





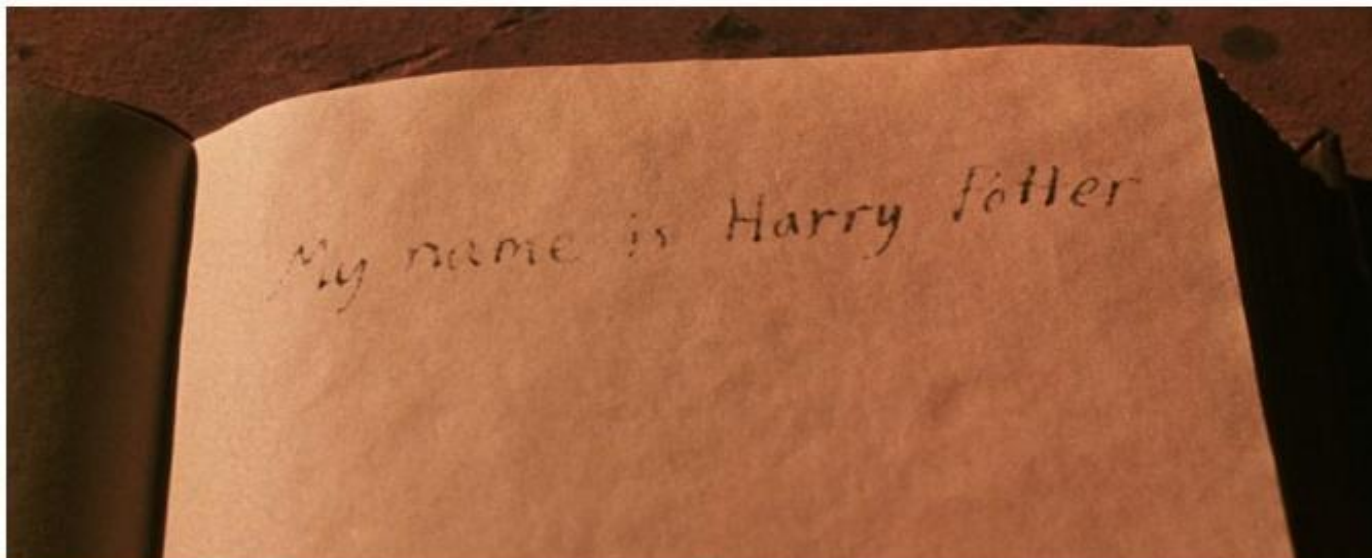
## ✓ Алгоритмы асимметричного шифрования

- RSA. Разработан в 1977 году в Массачусетском технологическом институте (США). Получил название по первым буквам фамилии авторов (Rivest, Shamir, Adleman). Криптостойкость основана на вычислительной сложности задачи разложения большого числа на простые множители.
- ElGamal. Разработан в 1985 году. Назван по фамилии автора - Эль-Гамаль. Используется в стандарте США на цифровую подпись DSS (Digital Signature Standard). Криптостойкость основана на вычислительной сложности задачи логарифмирования целых чисел в конечных полях.



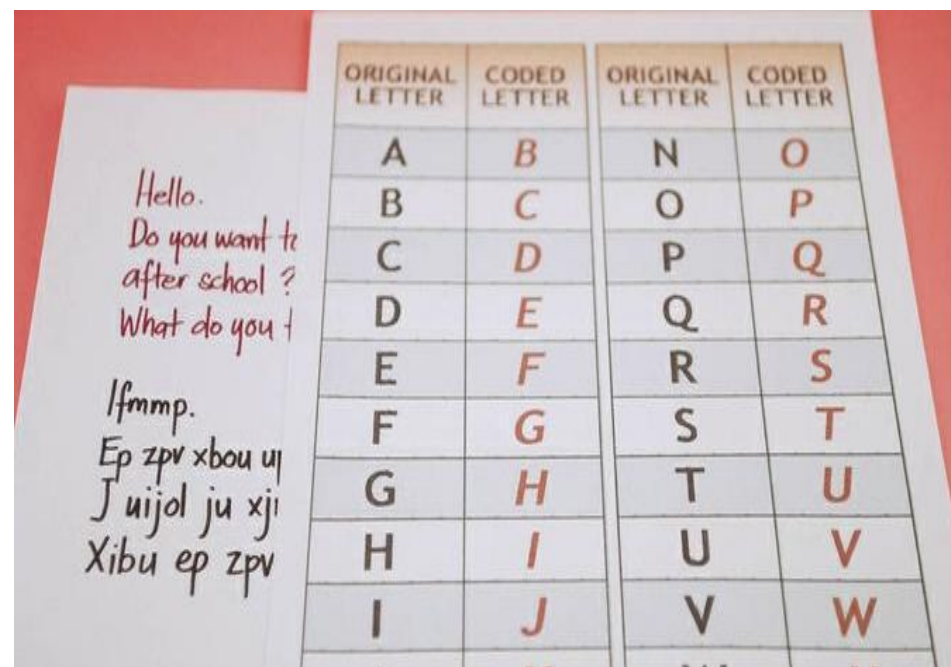
# Популярные коды и шифры.

- ✓ **Стеганография** — это искусство скрытого письма. Этой технике даже больше лет, чем кодам и шифрованию. Когда-то в Англии использовался такой метод: под некоторыми буквами на первой странице газеты стояли крохотные точки, почти невидимые невооруженным глазом. Если читать только помеченные буквы, то получится секретное сообщение! Была распространена практика уменьшения целых страниц текста до размера буквально одного пикселя, так что их было легко пропустить при чтении чего-то относительно безобидного.



✓ **ROT1.** Этот шифр известен многим детям. Ключ прост: каждая буква заменяется на следующую за ней в алфавите. Так, А заменяется на В, В на С, и т.д.

✓ **В настоящих кодах** каждое слово заменяется на другое. Расшифровывается такое послание с помощью кодовой книги, где записано соответствие всех настоящих слов кодовым



000 ↔ 110011

100 ↔ 000000

010 ↔ 100110

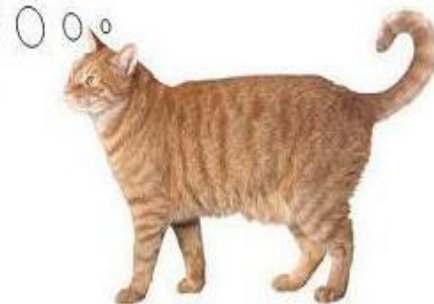
001 ↔ 010101

110 ↔ 001011

101 ↔ 101101

011 ↔ 011110

111 ↔ 111000



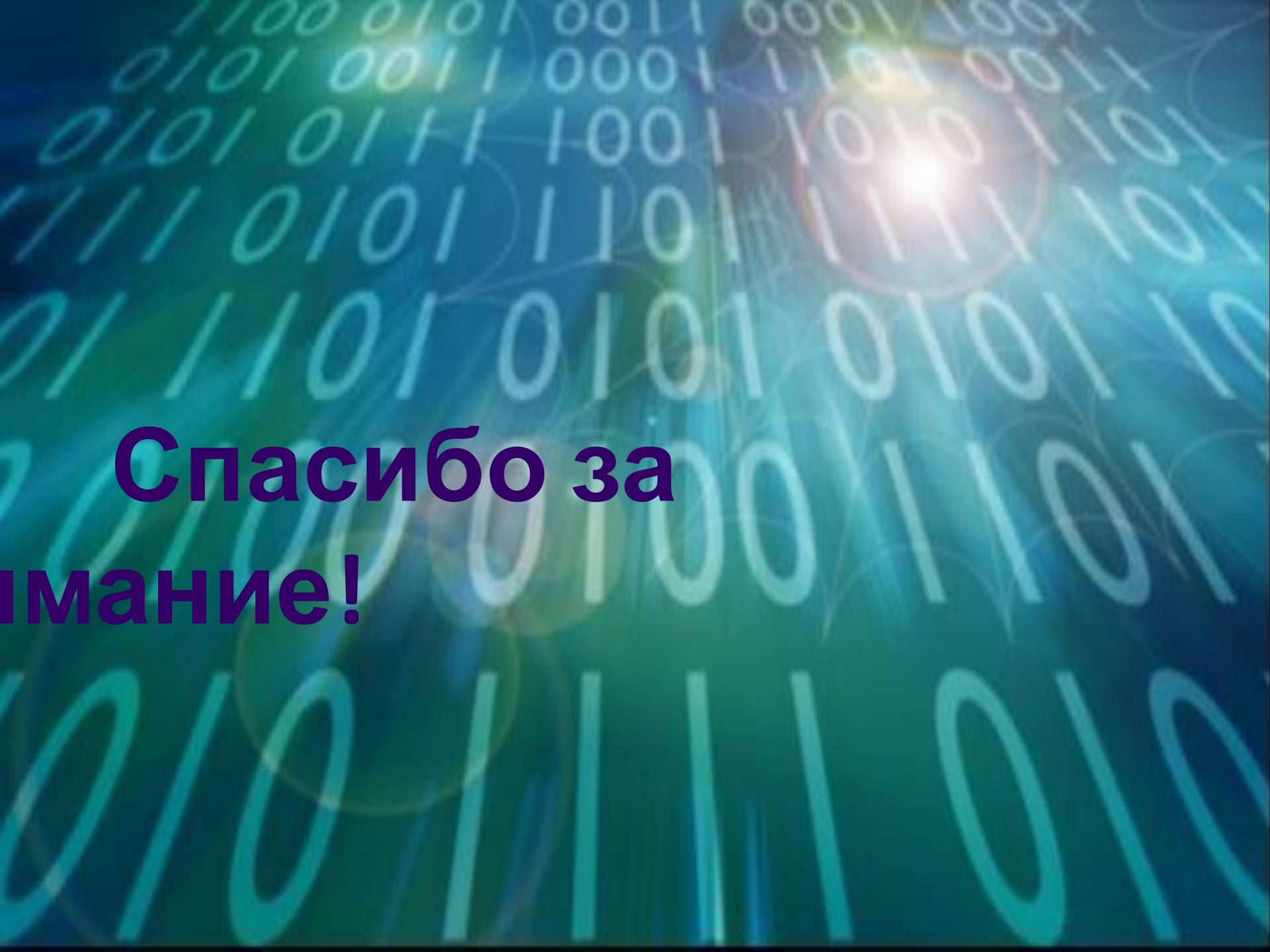


✓ **Неразгаданные: Криптос.** В 1990 году скульптура из 4 секций с нанесенными на них зашифрованными символами была установлена перед штаб-квартирой ЦРУ в качестве вызова для сотрудников агентства. 3 секции были расшифрованы, но четвертая уже 26 лет не поддается разгадке.

✓ **Шифр Билла.** В 1885 году в Вирджинии была анонимно опубликована небольшая брошюра, содержащая историю и три зашифрованных сообщения. История утверждает, что сообщения приведут к сокровищу, спрятанному человеком по фамилии Бил. С тех пор было расшифровано только одно из трех сообщений.



1, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263,  
38, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 20  
18, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304,  
4, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474  
50, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 82  
16, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59,  
14, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 17  
0, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 5  
4, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 7  
28, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 82  
1, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206  
5, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 9  
33, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36,  
34, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 46  
0, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 10  
1, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 24  
5, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 12  
48, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119  
16, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 1

The background is a dark blue gradient filled with glowing binary code (0s and 1s) in various sizes and orientations. A bright, multi-colored lens flare is positioned in the upper right quadrant, casting a soft glow over the scene.

**Спасибо за  
внимание!**