Cryptography

team_industr1al

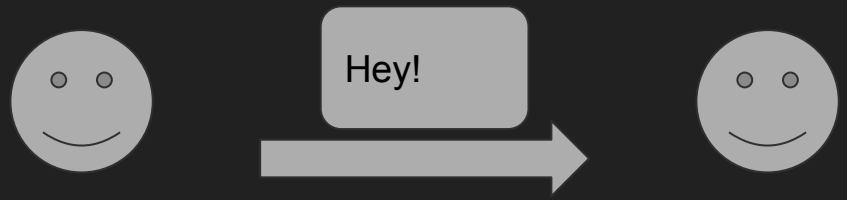
Content

1. Intro
2. (a)symmetric cryptography
3. Hashing
4. Complexity of breaking cipher or hash
5. Several attacks on ciphers
6. Where ciphers are used
7. Conclusion

Encryption

Alice & **B**ob

Mallory & Eve



team_industr1al

Why

1. Data security
2. Verifying the validity of data and its sources
3. Data integrity

team_industr1al

Symmetric Encryption

1. Шифр Цезаря
2. Шифр Виженера
3. Шифр Атбаш
4. Шифр Плайфаера
5. ADFGVX
6. XOR

Шифры основанные на сдвигах, перестановках

7. Шифр Вернама
8. IDEA
9. RC2
10. RC4
11. DES
12. Triple DES
13. Rijndael(AES)

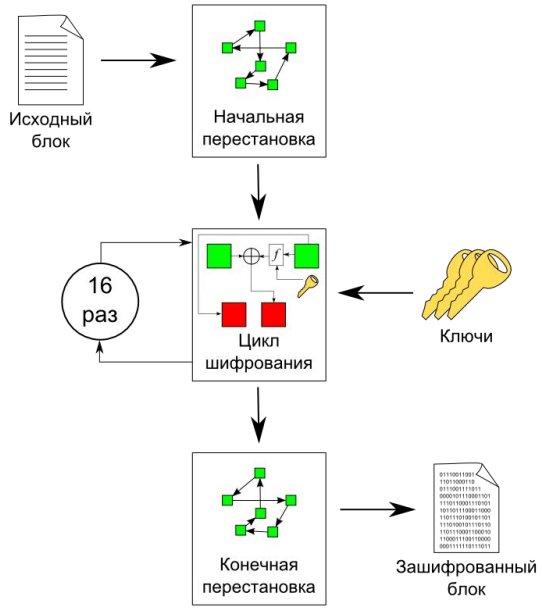
Блочные шифры

XOR

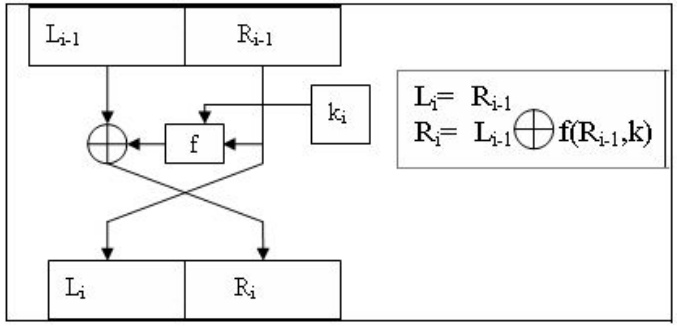
team_industr1al

Symmetric Encryption Examples

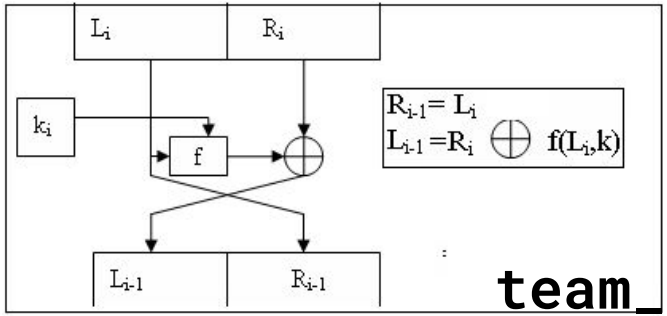
DES



Сеть Фейстеля (прямое преобразование)



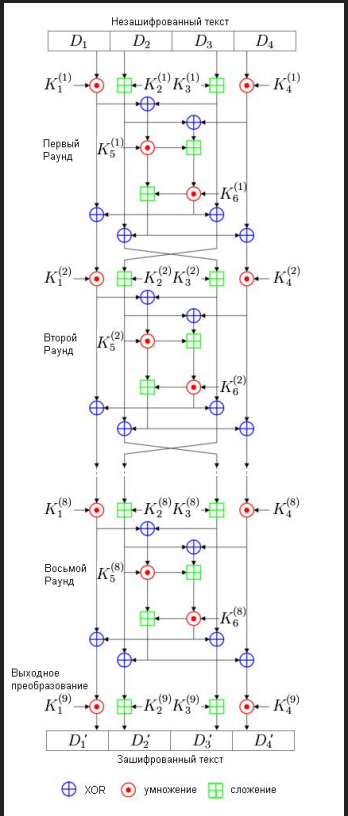
Сеть Фейстеля (обратное преобразование)



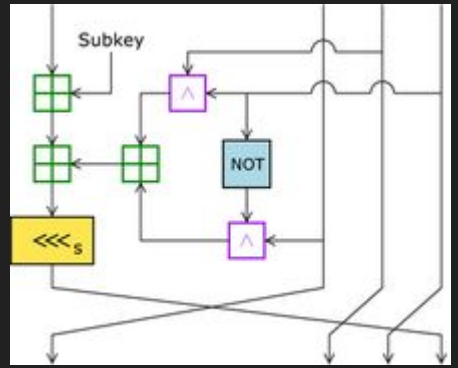
team_industr1al

Symmetric Encryption Examples

IDEA



RC2

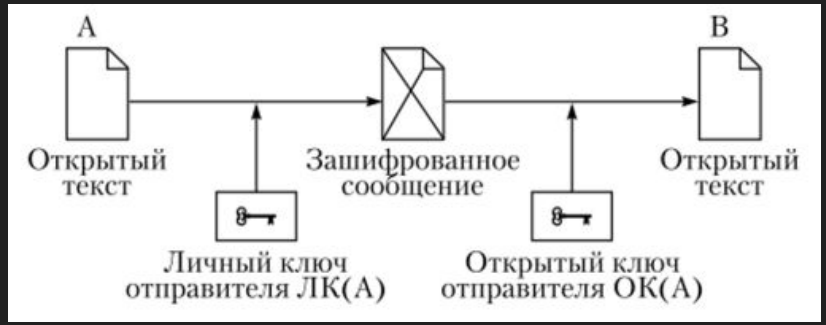


- быстрее DES
- блочный шифр с длиной блока 64 бита и переменной длиной ключа

team_industr1al

Asymmetric Encryption

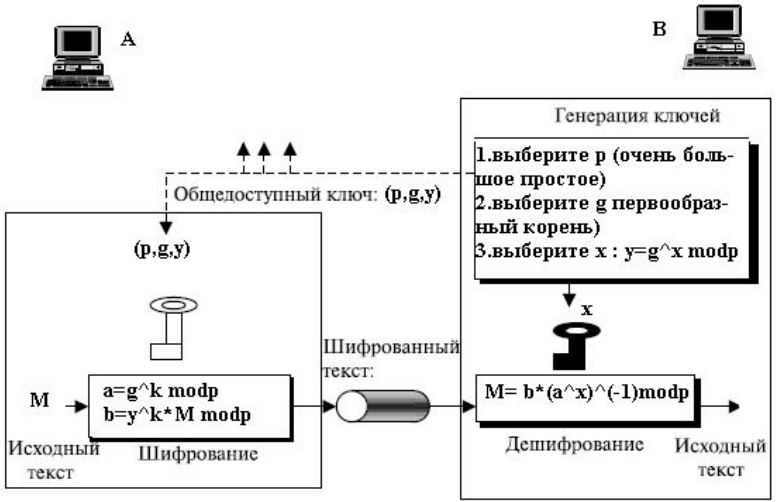
1. RSA (Rivest-Shamir-Adleman)
2. DSA (Digital Signature Algorithm)
3. Elgamal (Шифросистема Эль-Гамаля)
4. Diffie-Hellman Protocol
5. ECDSA (Elliptic Curve Digital Signature Algorithm)
6. ГОСТ Р 34.10-2012



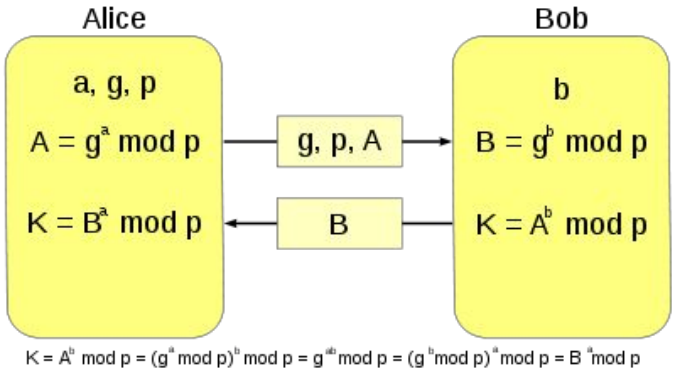
team_industr1al

Asymmetric Encryption Examples

Elgamal



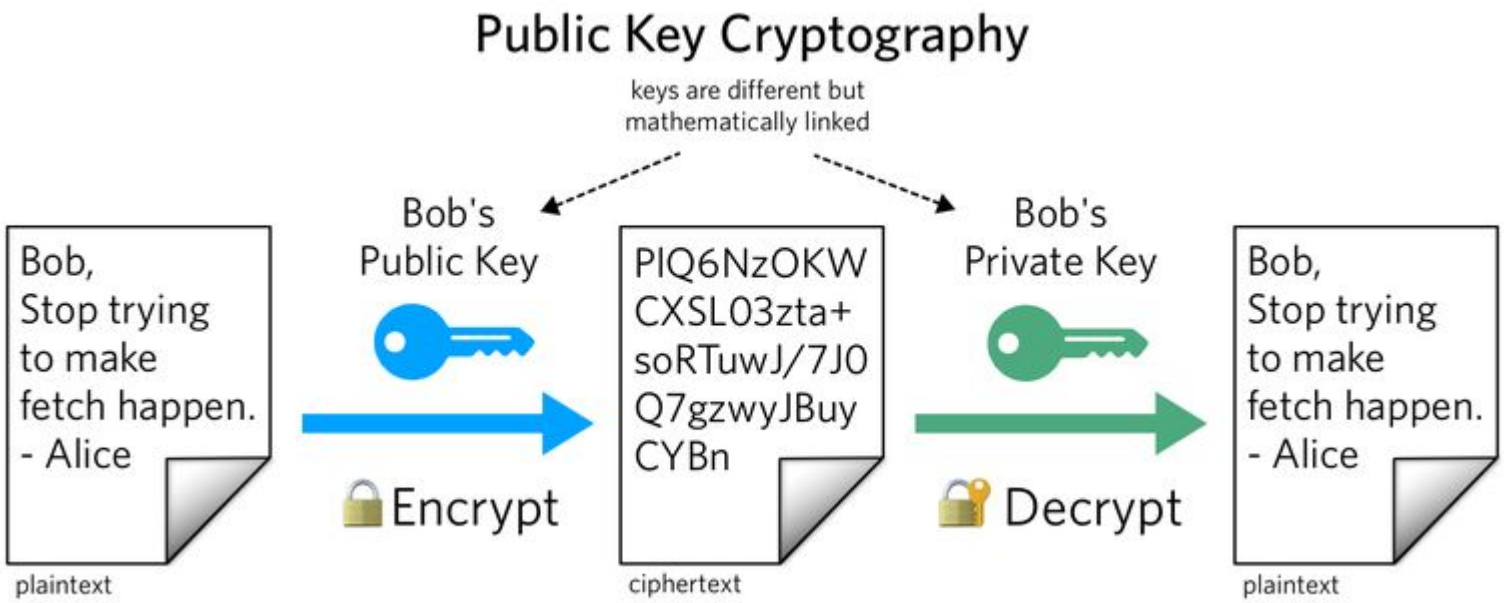
Diffie-Hellman



team_industr1al

Asymmetric Encryption Examples

RSA



team_industr1al

Hashing

Plain Text

Hashed Text

Привет! → 5797a339206d7d7d5aeb2903d7114867

team_industr1al

Complexity of breaking hash

$$\overbrace{\text{SHA256}}^{\text{Cryptographic hash function}}(\text{“}\underbrace{\qquad\qquad}_{???}\text{”}) = \underbrace{\begin{array}{l}10011111001111000101111001001011\\11011110111011010011011010100101\\01010100010001011110111011010010\\10000101011100101100110011111101\\00111001000111000001011001100001\\00110010101100111110101100100100\\00010101011010001010001000010010\\11000001100001111001001110000100\end{array}}_{\text{Desired output}}$$

$$\left.\begin{array}{l}00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000000000000\\00000000000000000000000110001110\end{array}\right\} 2^{256} \text{ possibilities}$$

youtu.be/watch?v=S9JGmA5_unY

team_industr1al

Complexity of breaking cipher

Задача дискретного логарифмирования

$$a^x = b(mod\ m),$$

где a и m известны и взаимно просты (не имеют общих делителей), b также известно.

https://e-maxx.ru/algo/discrete_log

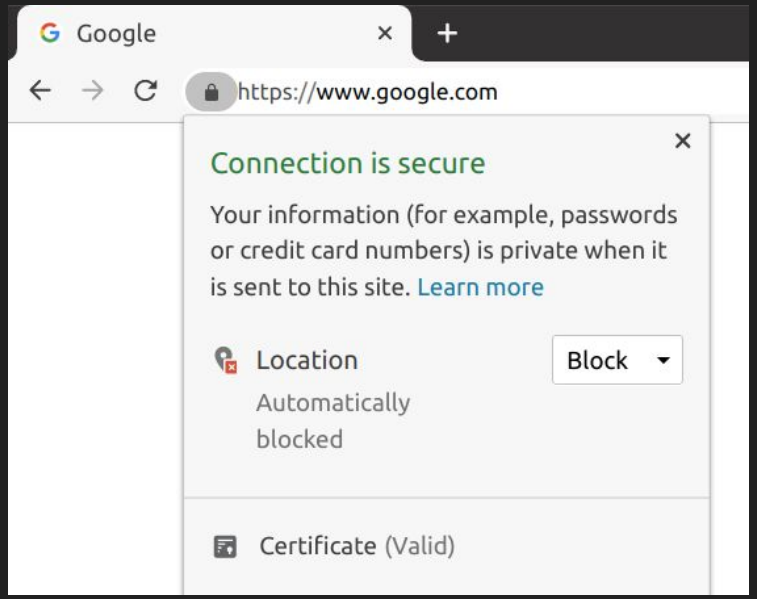
team_industr1al

Several attacks on ciphers

Attack:	Defence:
Man In The Middle	Holding Hands Protocol
Bruteforce	Complex dictionary

team_industr1al

Where ciphers are used



Mobile Networks

team_industr1al

Tools for CTF tasks

https://github.com/Ciphey/Ciphey

https://gchq.github.io/CyberChef/

https://github.com/Ganapati/RsaCtfTool/blob/master/RsaCtfTool.py

Sources

Book

team_industr1al

team_industr1al

github.com/ilyas-mspv

Questions?

End-to-end Encryption

1.