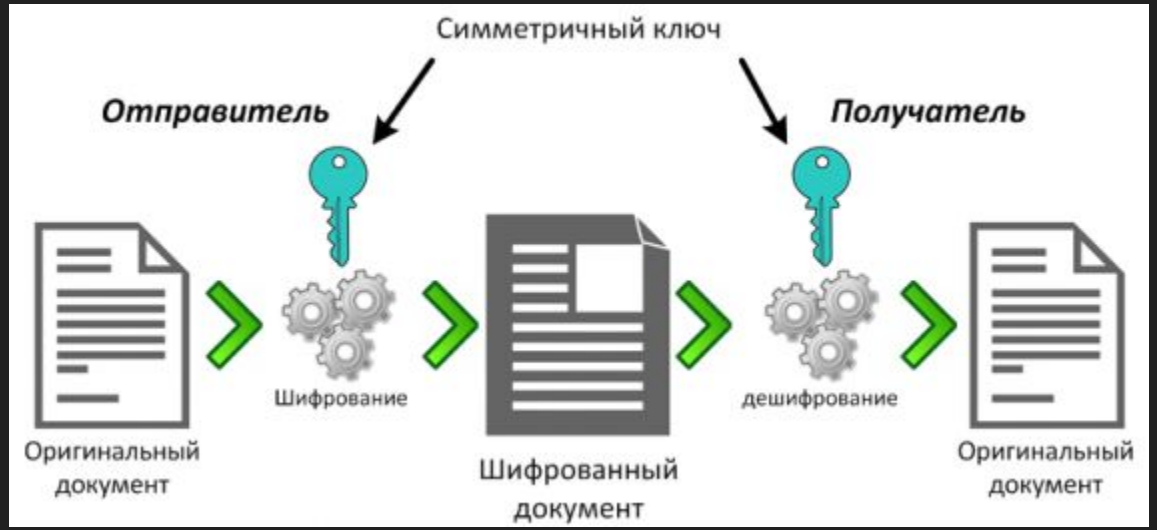
CTF на Физтехе

Занятие 6

Симметричное шифрование

- Для шифрования и расшифровки используется один и тот же ключ



DES

- Data Encryption Standard
- Разработан IBM в 1970-ых
- Размер блока - 64 бита
- Длина ключа - 56 бит (+ 8 бит для проверки целостности)
- Сейчас является небезопасным

Атаки на DES

- Полный перебор ключей (brute force) (на современных ПК займет ~200 дней)
- В 1997 RSA Laboratories запустили DES Challenge
- DES Challenge I = 96 days (1997)
- DES Challenge II-1 = 39 days (1998)
- DES Challenge II-2 = 56 hours (1998)
- DES Challenge 3 = 23 hours (1999)

AES

- Advanced Encryption Standard (aka Rijndael)
- Принят новым стандартом по результатам конкурса NIST в 2001
- Размер блока - 128 бит
- Длина ключа - 128, 192 или 256 бит
- Активно используется

Атаки на AES

- Ничего значительно лучше перебора пока не придумали
- Side-Channel атаки
  - Timing attack
  - Атаки по энергопотреблению

Другие симметричные блочные шифры

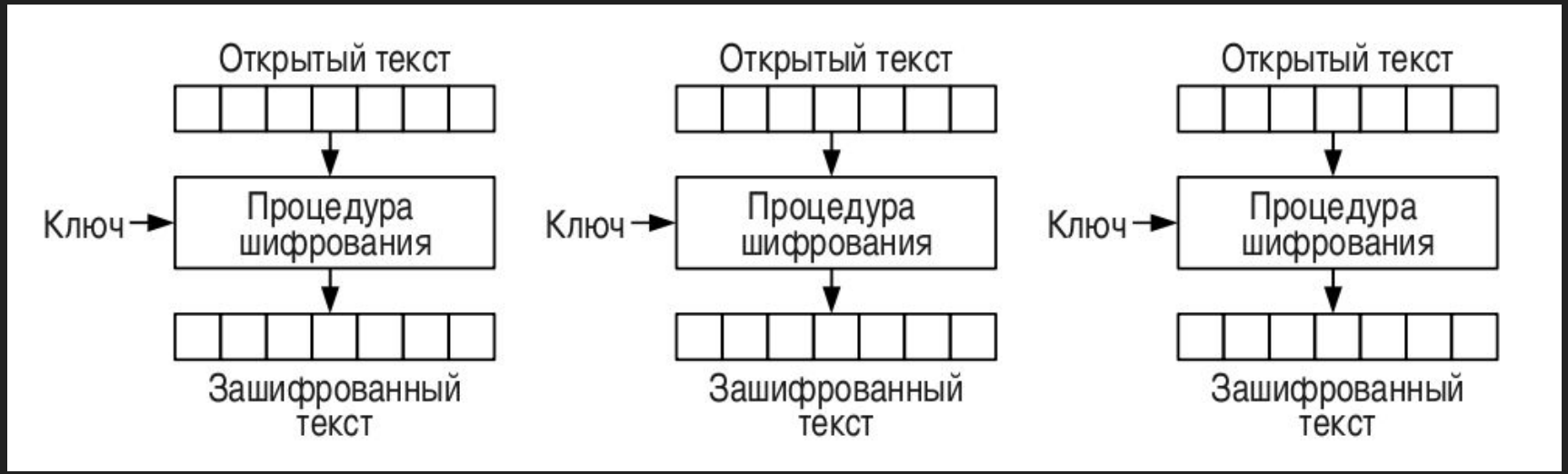
- Triple DES
- RC4 - главная дыра в протоколе WEP
- RC5
- RC6
- Кузнечик (ГОСТ Р 34.12-2015)
- Blowfish

Общий алгоритм шифрования

- Дан P = plaintext, с некоторой длиной L = len(P)
- Используем Padding алгоритм для получения длины, кратной размера блока (Zero padding, PKCS #7, ANSI X.923, ISO 10126, ISO/IEC 7816-4)
- На полученный текст используем алгоритм потокового шифрования (ECB, CBC, CFB) с выбранным блочным шифром

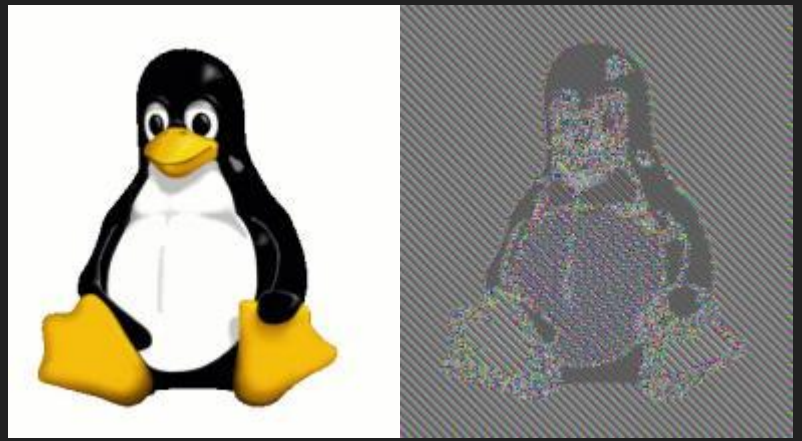
EBC

- Electronic code book



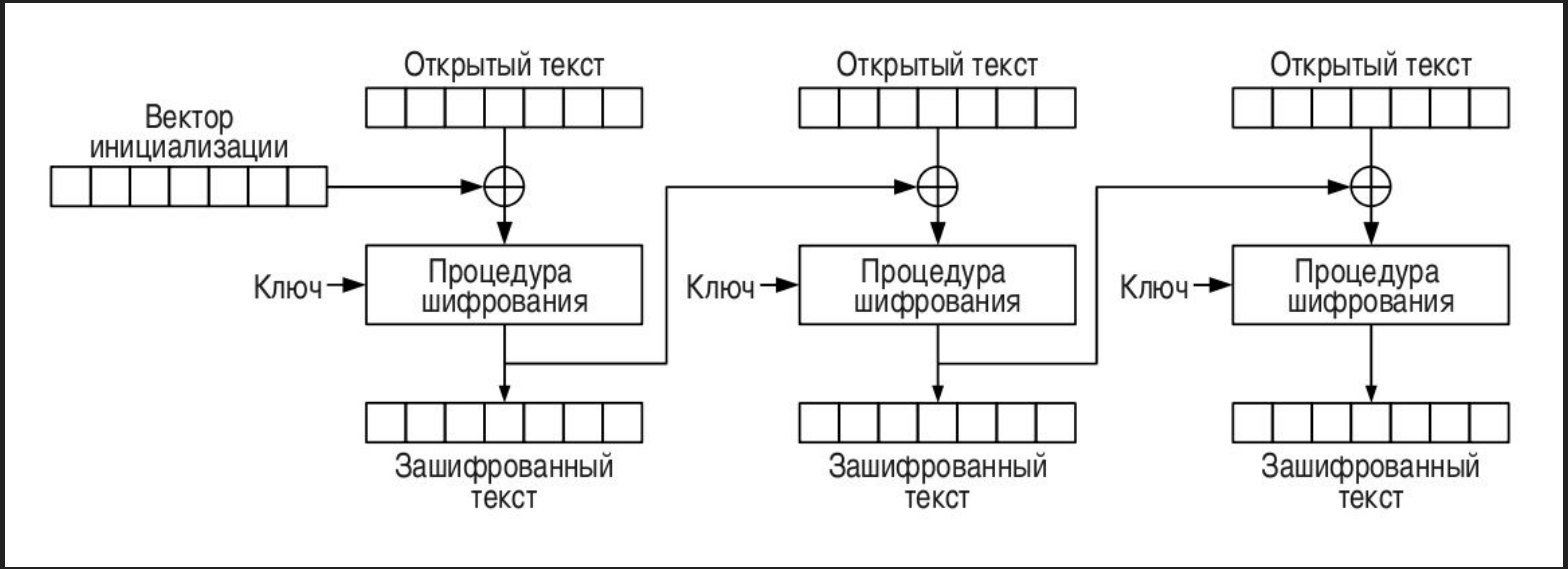
Проблемы ECB

- При искажении/замене одного блока шифротекста, искажается только этот блок открытого текста
- Возможные атаки связанные с заменой блоков



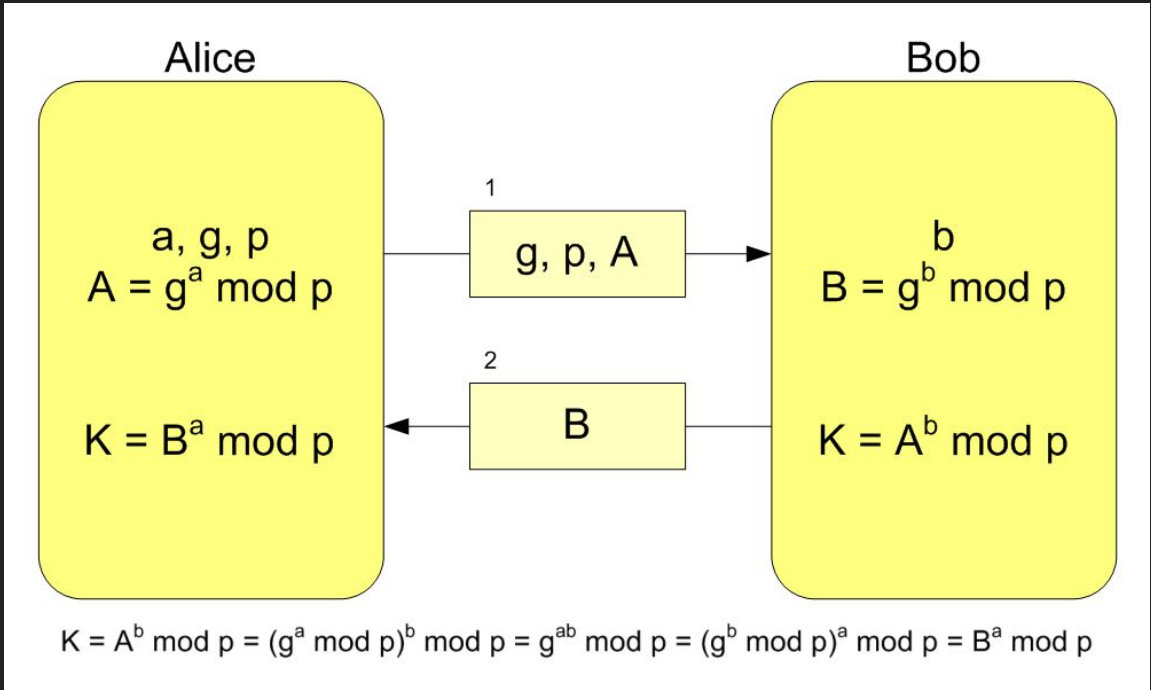
CBC

- Cipher block chaining
- Кроме ключа есть еще IV (Initialization vector), может быть как частью ключа, так и открытой информацией



Протокол Диффи-Хеллмана

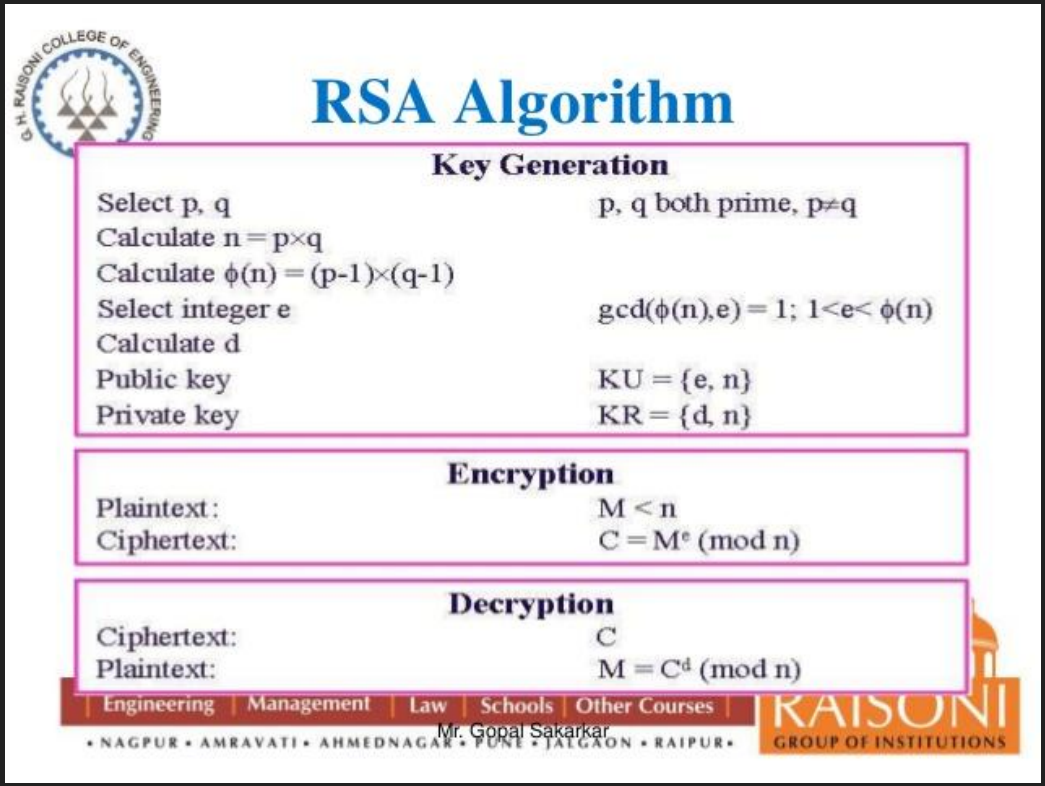
- Способ обменяться ключами по открытому каналу



Асимметричное шифрование

- Для шифрования и расшифровки используются различные ключи
- Открытый ключ известен всем и используется для шифрования
- Приватный ключ хранится в секрете и используется для расшифровки
- По открытому ключу нельзя(вычислительно сложно) получить приватный ключ

RSA


G. H. RAISONI COLLEGE OF ENGINEERING
RSA Algorithm
Key Generation
Select p, q
p, q both prime, p≠q
Calculate n = p×q
Calculate ϕ(n) = (p-1)×(q-1)
Select integer e
gcd(ϕ(n),e) = 1; 1<e< ϕ(n)
Calculate d
Public key
KU = {e, n}
Private key
KR = {d, n}
Encryption
Plaintext:
M < n
Ciphertext:
C = M^e (mod n)
Decryption
Ciphertext:
C
Plaintext:
M = C^d (mod n)
Engineering | Management | Law | Schools | Other Courses
• NAGPUR • AMRAVATI • AHMEDNAGAR • PUNE • JALGAON • RAIPUR •
RAISONI
GROUP OF INSTITUTIONS
Mr. Gopal Sakarkar

Вопросы?