

# Защита информации в корпорациях

- Прозрачное шифрование
- Системы аутентификации
- Комплексные решения

*Криптосистема* — {шифрование, дешифрация}

*Секретный ключ* - параметр алгоритма шифрования

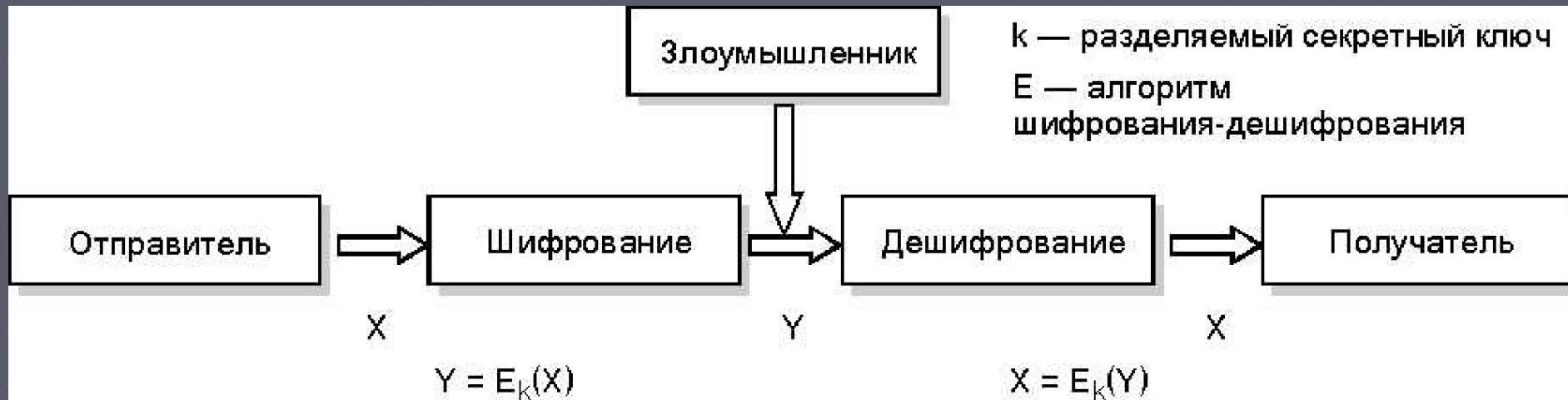
## **ПРАВИЛО КЕРКХОФФА**

**стойкость шифра должна определяться только секретностью ключа**

Два типа криптосистем:

- (1) симметричные
- (2) асимметричные

# Симметричное шифрование



в 1949 г. Клод Шеннон

# Недостатки симметричного шифрования

- ◆ Критичны к надежности канала передачи ключа
- ◆ Плохая масштабируемость схемы распределения ключей. Требуется  $n(n-1)/2$  ключей
- ◆ Проблема генерации криптостойких ключей (56 бит)

# Advanced Encryption Standard (AES)

## Новый стандарт

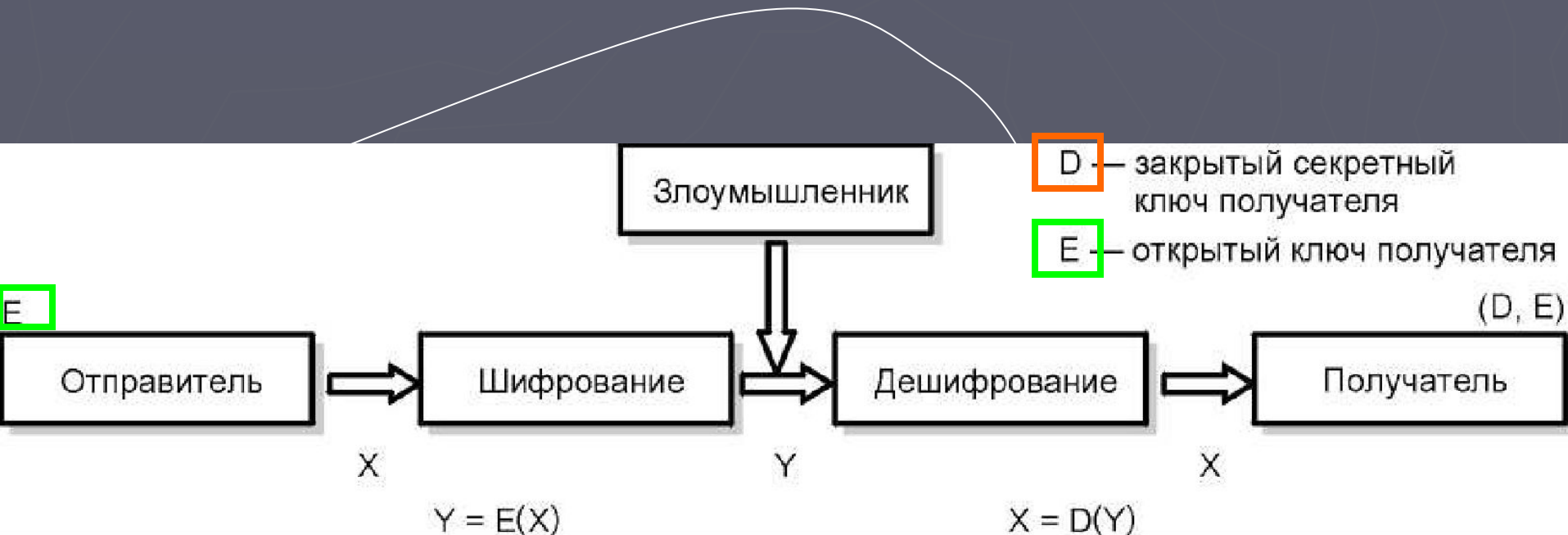
- лучшее сочетание безопасности и скорости, чем у DES
- 128-разрядные ключи, может поддерживать 192- и 256-разрядные ключи (vs 56 DES).
- за каждый цикл кодирует блок 128 бит (vs 64 DES)
- получит статус федерального стандарта по обработке информации летом 2001 года

## Процесс перехода:

- (1) прост для настраиваемых продуктов
- (2) проблемы с унаследованными алгоритмами шифрования (в браузерах – RC4, в электронной почте PGP – IDEA)

# Несимметричное шифрование

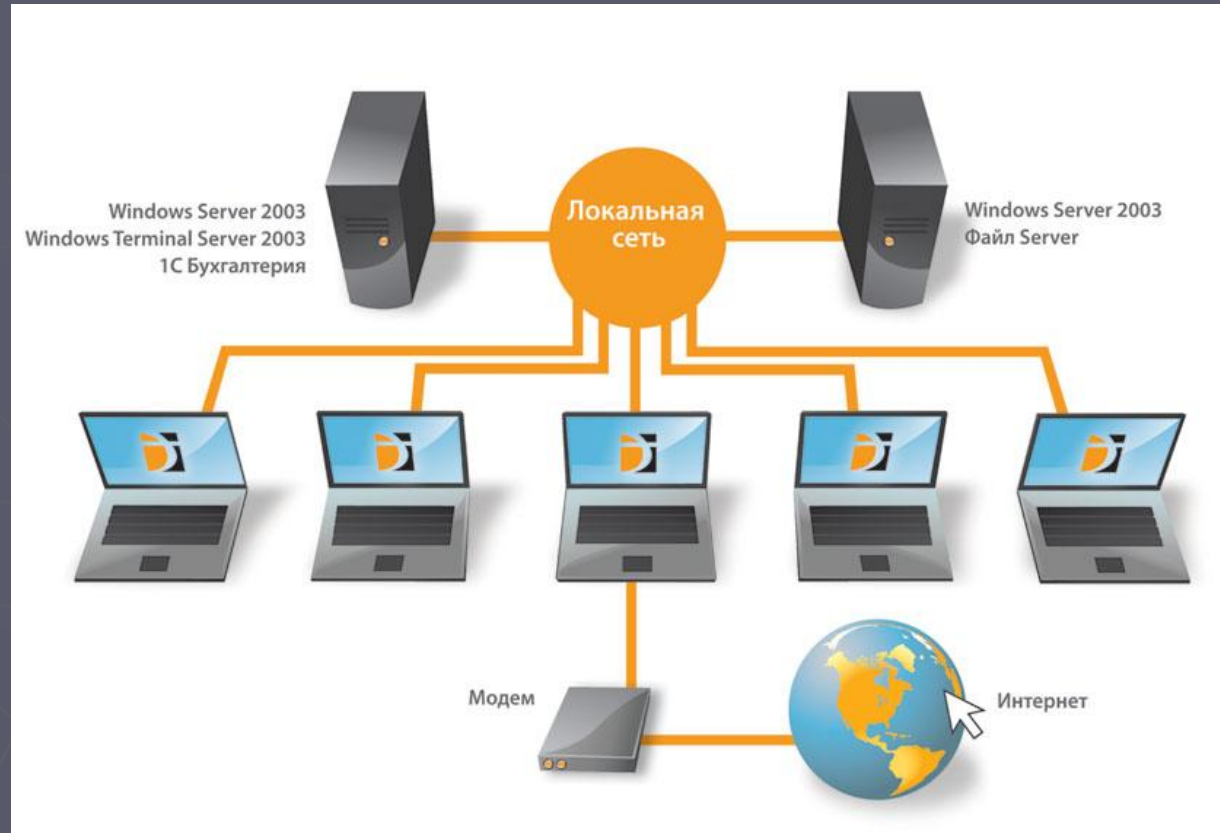
В середине 70-х—Диффи и Хеллман



# Архитектура сегодня

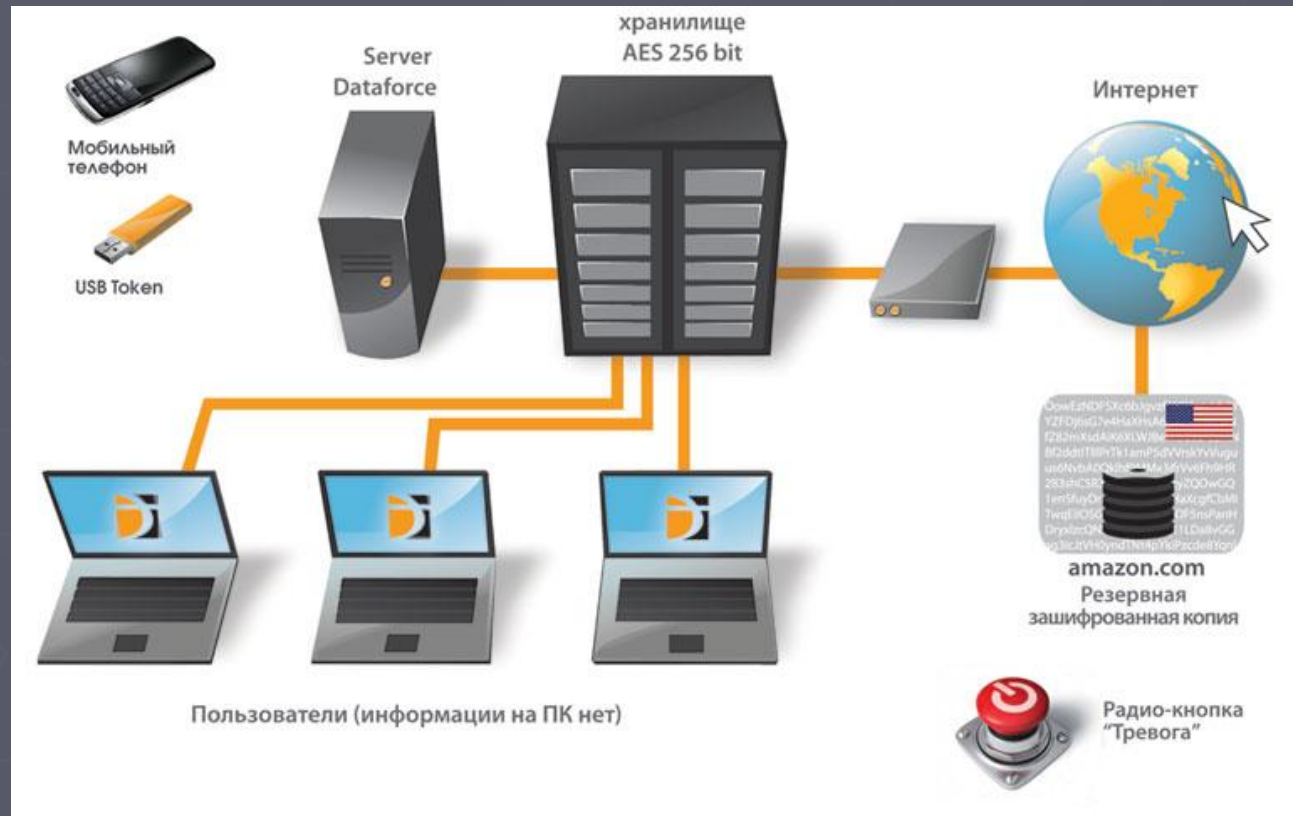
## Локальная сеть:

- ▶ Кража / повреждение / изъятие ПК влечет потерю всей информации. Резервной копии нет.
- ▶ Злоумышленник получает доступ ко всей информации
- ▶ Любой сотрудник имеет доступ к информации через локальную сеть.



# Архитектура с защитой

- ▶ Постоянно защищенные данные алгоритмом AES 256 бит
- ▶ Включение доступа только через Token, или сотовый телефон директора
- ▶ Резервная копия в какой либо стране (например США)
- ▶ Радио-кнопка «тревога» в офисе

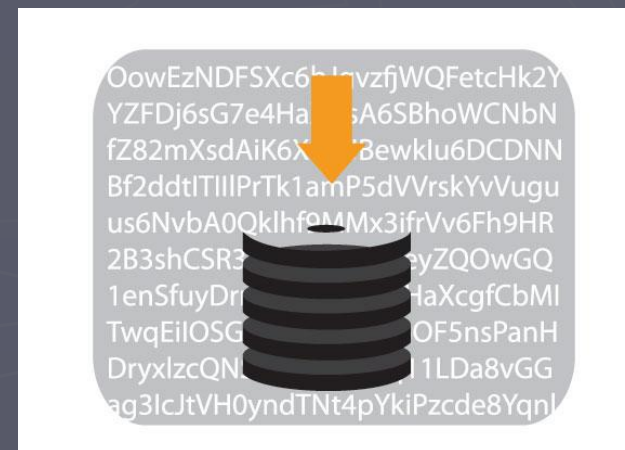




# Шифрование на лету

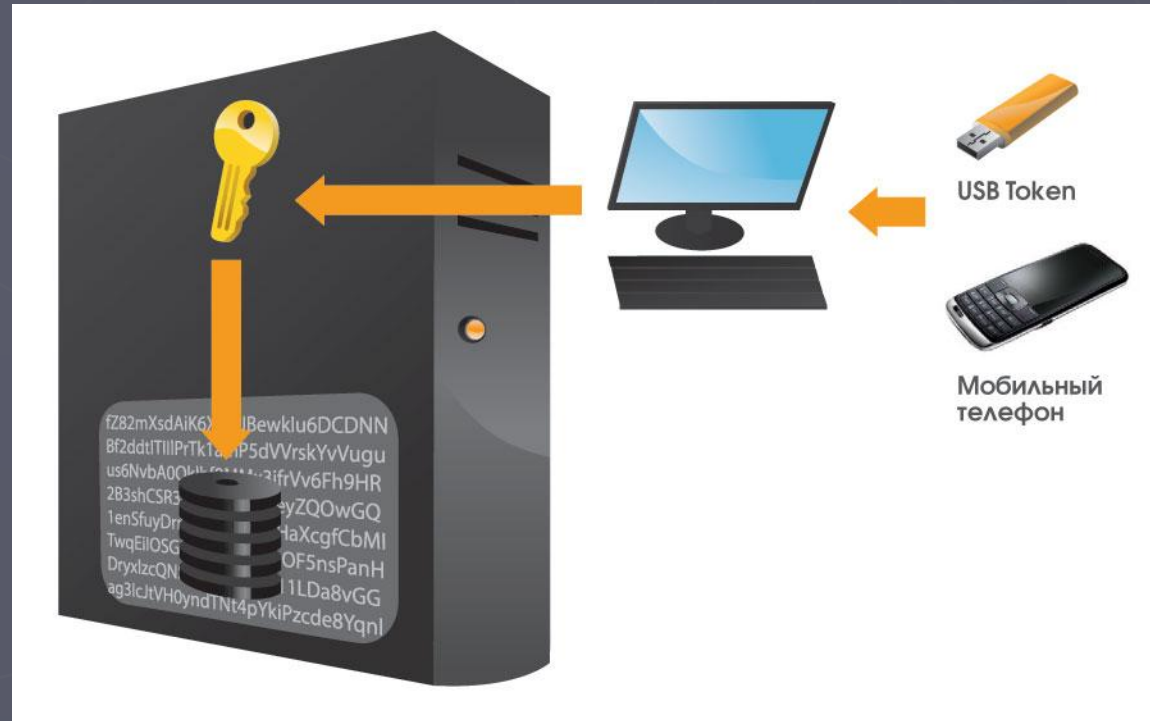
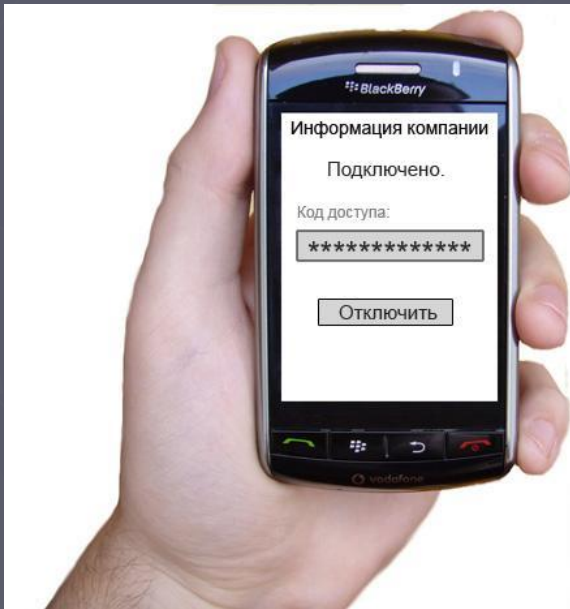
На дисках информация хранится в постоянно зашифрованном виде:

G1iQwiDSAAPVfOXMAIqIX7HIYxcT47BMOIV3oI6gGbKgXml6M  
w6VB4GShZR15PRoEUqGD9tHKV2kZFT0gTinApMQxoWmvJdt  
6NonMuoYppIhEVHrUFwIS0ixorohXOmFuV7HhBch71ytZA2UFC  
qfuYbCvgS7UAxv9EEssJE8IZLzyXsojIBROh06ESvd2GZJp4sTU  
XIX52ryXp3eV2YWFTtzFpMyor0gzXELxVUC4WoV5UXhEeQYZ  
KHHoWw0GCy4adoTBzDlvYrDjDqUgwBxUsateJTWyZSmLzetP  
PD1up1f1uOYc6BgkFUiyxD00q5fXrvfBtv8FmkkJ8ZrHBfdtaDcq6l  
7MCb91JAKnGkODgCiv1ZMqmNHcbjCIPYVdjQCeO14I4Auz5dO  
Z3Qx82ewwe9ECtq9N2oEbigYIWAYByQFMhbbEK4FXtnlxOhF  
wup4kAeL98iBGeyZt9sDirml9DWJ0H31P07I57miy1hGa7xzwIQN  
Y4kN2AvSTyV4PrRiHQUryESTBbmw7Vt0Nkros3EjvPPfQtkrb9c  
cOHYUrzo8SqhHDxfFPBRL9WcEzoXdiKdDa1WrMwyDxMX0h  
Wv9NICUNRRuj9YqwR8sWZfL6J9nYUBtl99alMEFtZxMcwsSIRa  
Eeqq5Lh1c2IcCn81bTtF5MPEFOzloJ7kzLpTTuZPzoroXNuSolJ0  
AxBUy4tGhTXjjUZ51GnYonF3hizmOTUDUsO0jom0HxO1qRPIO  
PloyWopMSvgrMaGaBGBpk9HpieyQVJx6czeuh84KBjnpfHu7JjR  
iRgjbXLepbg7FwWLI4Ilfktz3Awe9jV2XHSh00IABWfh2i6KhRNx  
DuHQa5wgsZlbfKGUVKP7Bf7Q3Nj3C8kTSmmXakV5tVESn8R  
HrPqfVKNxmczgcLUpuE3hRhZmW7HljM8F3hPLbel1PT0MBAmj  
ulOhRjSS2n1I9BO7KUZXHho0s0htefsZNuZrl14lpdmmnxmP1Ek  
o2liGA9q6Lip3ObhO8NIgO6cNfCYEwYTLQRBRTgeb



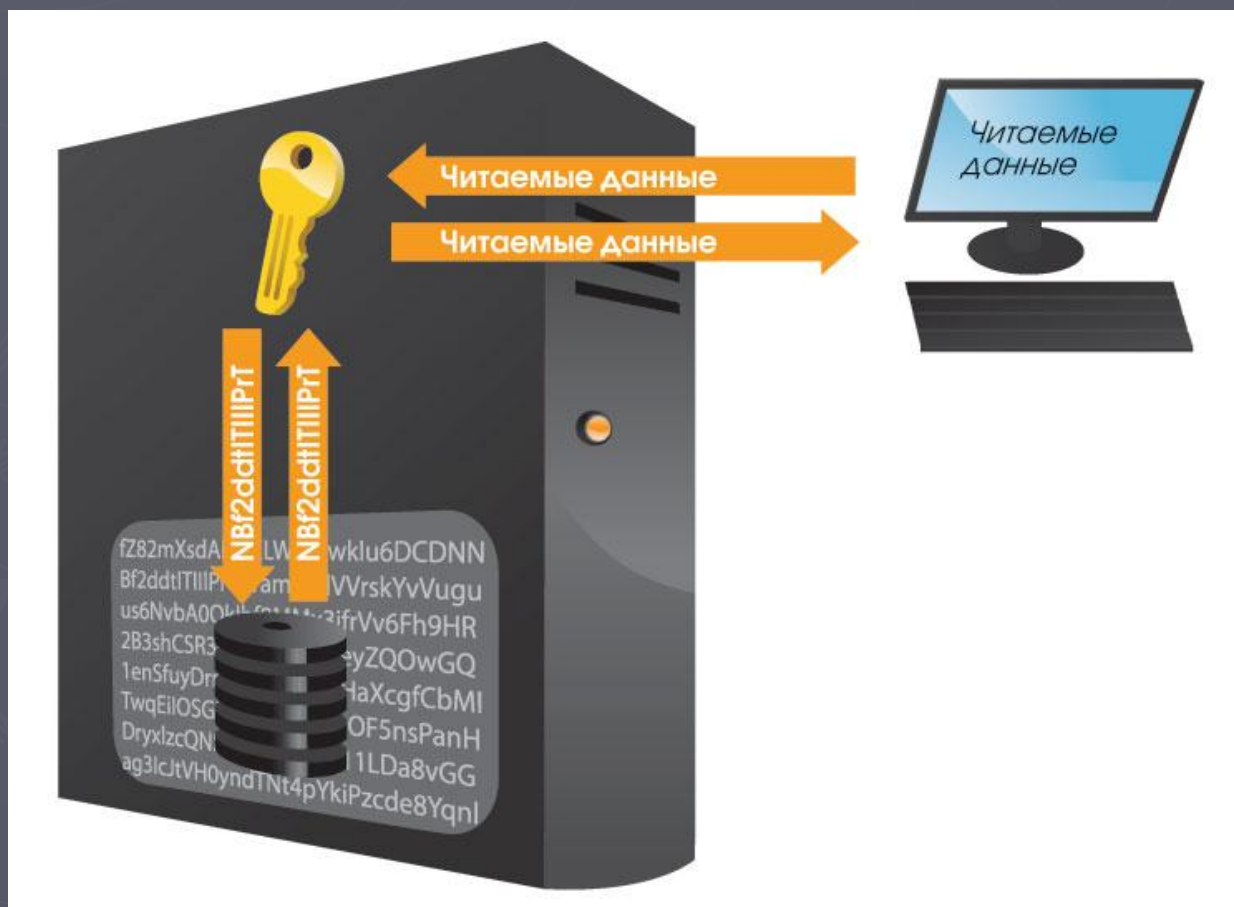
# Шифрование на лету

Стоит только ввести ключ шифрования с помощью токена, смарт карты или телефона:



# Шифрование на лету

Вся зашифрованная информация  
становится доступной



# Шифрование на лету

При появлении тревоги, нажмите кнопку



# Шифрование на лету

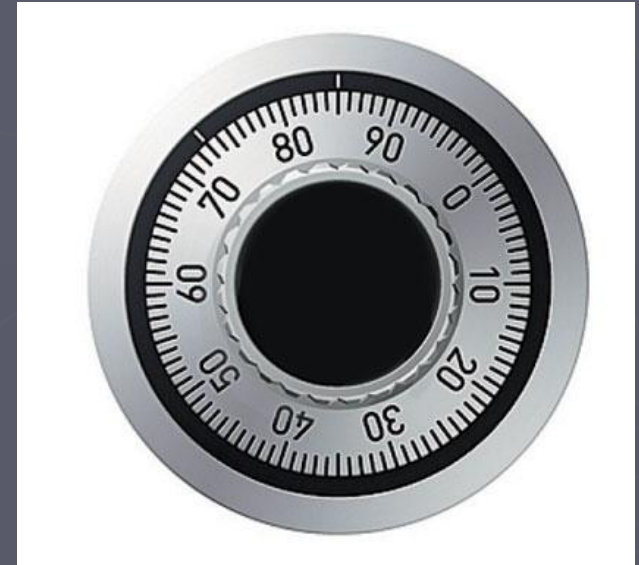
Нет ключа- нет информации



# Насколько это надежно?

**Advanced Encryption Standard (AES)** — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит),

**принятый в качестве стандарта шифрования правительством США**



**Ключ длиной 256 бит:**

**A4bB0sth3z6Dz12vlvoNMidl1FTfEW7GbbzLT95jOvo7suD3pCs5XISd**

**Подбирается  $2 \cdot 10$  в 14 степени лет, современными ПК**