ВОПРОСЫ БЕЗОПАСНОСТИ

Аспекты безопасности:

* предупреждающая безопасность (forward secrecy) — безопасная генерация ключей сеанса (алг. Д.–Х.);

* аутентичность сторон — инфраструктура открытых ключей (PKI) на основе несимметричных криптоалгоритмов;

* конфиденциальность данных — шифрование при помощи симметричных криптоалгоритмов;

* целостность данных — имитовставка на основе хэшей (HMAC);

* электронная цифровая подпись.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Алгоритм Диффи — Хеллмана — Меркля (1976)

Параметры алгоритма: p — большое простое число и g — первообразный корень по модулю p ($\exists x \in \mathbb{N}$ для $\forall a \in [1;p-1]$: $g^x \bmod p = a$).

DH-g1 (RFC 2409) — $p \sim 2^{1024}$ (π«958), $g=2$; DH-g14 (RFC 3526) — $p \sim 2^{2048}$ (π«1982), $g=2$.
$p=2q+1$ (числа Софи Жермен), q — «порядок подгруппы»

C: генерирует случайное число a ($a<q$), вычисляет $A=g^a \bmod p$, отсылает A серверу

S: генерирует случайное число b ($b<q$), вычисляет $B=g^b \bmod p$, вычисляет общий секрет $K=A^b \bmod p$ ($\equiv g^{ab} \bmod p$), отсылает B клиенту

C: вычисляет общий секрет $K=B^a \bmod p$ ($\equiv g^{ab} \bmod p$)

Стойкость алгоритма основана на вычислительной сложности задачи *дискретного логарифмирования*: решение уравнения $g^a \bmod p = A$ относительно a при известных g, p, A.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Алгоритм Диффи — Хеллмана — Меркля (1976)

Пример:
$p = 23$ ($q = 11$), $g = 5$

C: генерирует случайное число $a = 6$, вычисляет $A = 5^6 \bmod 23$, отсылает $A = 8$ серверу

S: генерирует случайное число $b = 10$, вычисляет $B = 5^{10} \bmod 23$, вычисляет общий секрет $K = 8^{10} \bmod 23 = 3$, отсылает $B = 9$ клиенту

C: вычисляет общий секрет $K = 9^6 \bmod 23 = 3$

Злоумышленник может получить $p = 23$, $g = 5$, $A = 8$, $B = 9$.
Чтобы вычислить a, b, K из уравнений $8 = 5^a \bmod 23$ и $9 = 5^b \bmod 23$, надо перебрать все числа от 1 до 11.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

RSA (Ron Rivest, Adi Shamir, Leonard Adleman – MIT, 1977)

Несимметричный криптоалгоритм, используется для шифрования и генерации цифровых подписей.

Генерация ключа:

Выбираются два больших случайных простых числа p и q ($\sim 2^{1024}$). $n=pq$ — «модуль». $f=(p-1)(q-1)$. Выбирается «открытая экспонента» e ($1<e<f$) взаимно простая с f (обычно e=65537). Вычисляется «секретная экспонента» d мультипликативно обратная к e по модулю f: $de \bmod f = 1$. Открытый ключ: (e,n). Закрытый ключ: (d,n).

Шифрование — дешифрация:

M — исх. сообщение ($0<M<n-1$), C — шифр.

Шифрование: $C = M^e \bmod n$. Дешифрация: $M' = C^d \bmod n$.

Стойкость алгоритма основана на вычислительной сложности разложения n на простые множители («задача RSA»).

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

RSA (Ron Rivest, Adi Shamir, Leonard Adleman – MIT, 1977)

Пример:
$n = 11 \cdot 13 = 143$; $f = 10 \cdot 12 = 120$;
$e = 113$ (у 113 и 120 нет общих делителей);
$d = 17$ ($17 \cdot 113 \bmod 120 = 1$);
Открытый ключ: (113, 143). Закрытый ключ: (17, 143).

Исходное сообщение: $M = 123$.
Шифрование: $C = M^e \bmod n = 123^{113} \bmod 143 = 41$
Дешифрация: $M' = C^d \bmod n = 41^{17} \bmod 143 = 123$

Злоумышленник знает: $M^{113} \bmod 143 = 41$ (перебор M от 0 до n-1)
Не зная разложения n на простые множители p и q, злоумышленник не может вычислить d из: $d \cdot 113 \bmod (p-1)(q-1) = 1$.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Симметричные криптоалгоритмы

* *Поточные шифры* — шифрование проводится над каждым битом исходного текста с использованием *гаммирования* (псевдослучайная последовательность, характеристики которой определяются ключом шифра, при помощи XOR накладываются на исходный текст).
Примеры: RC4, SEAL, Trivium, Rabbit

* *Блочные шифры* обрабатывают исходный текст по блокам определённой длины, применяя несколько циклов (*раундов*) преобразования (раундовых функций). Обычно в каждом раунде свой ключ, получаемый из первоначального ключа.
Сети Фейстеля.
SP-сети.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

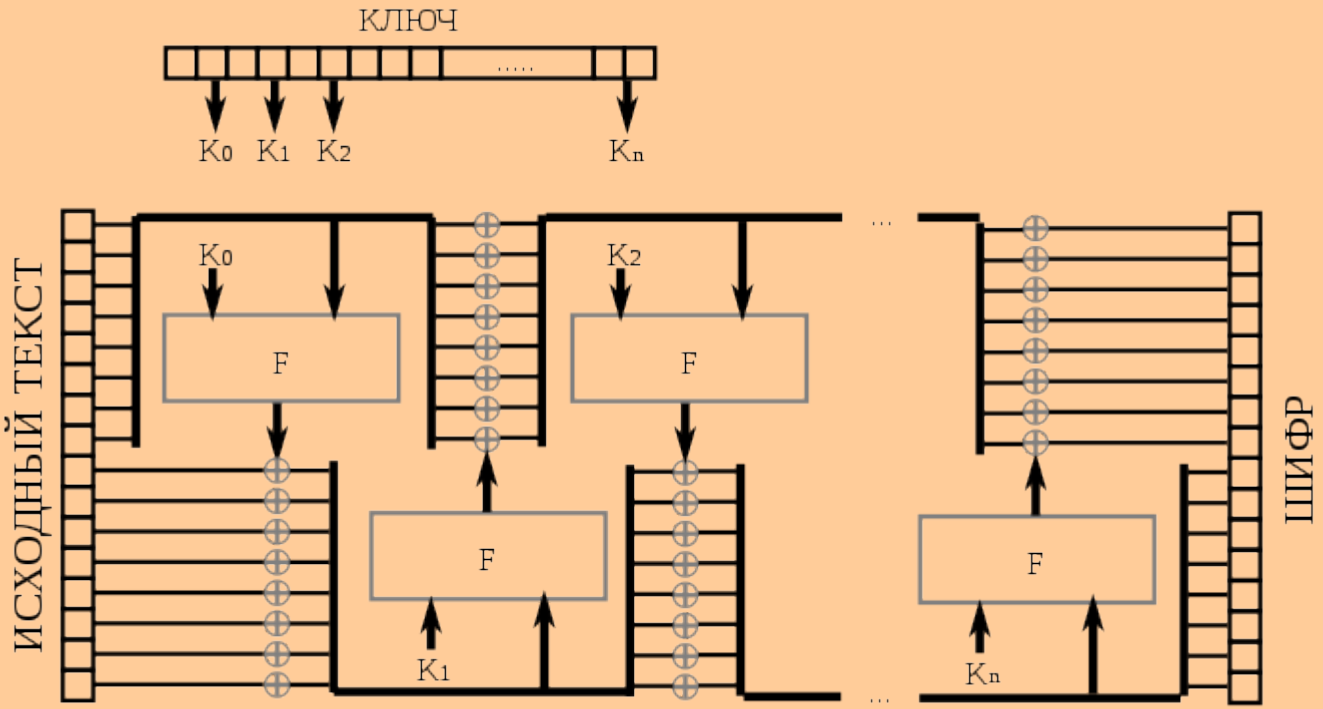
ВОПРОСЫ БЕЗОПАСНОСТИ

Симметричные криптоалгоритмы

Блочные шифры — сети Фейстеля

Раундовая функция *F* — нелинейна по отношению к XOR, имеет лавинный эффект

Примеры: DES, ГОСТ 28147-89, IDEA, CAST



© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

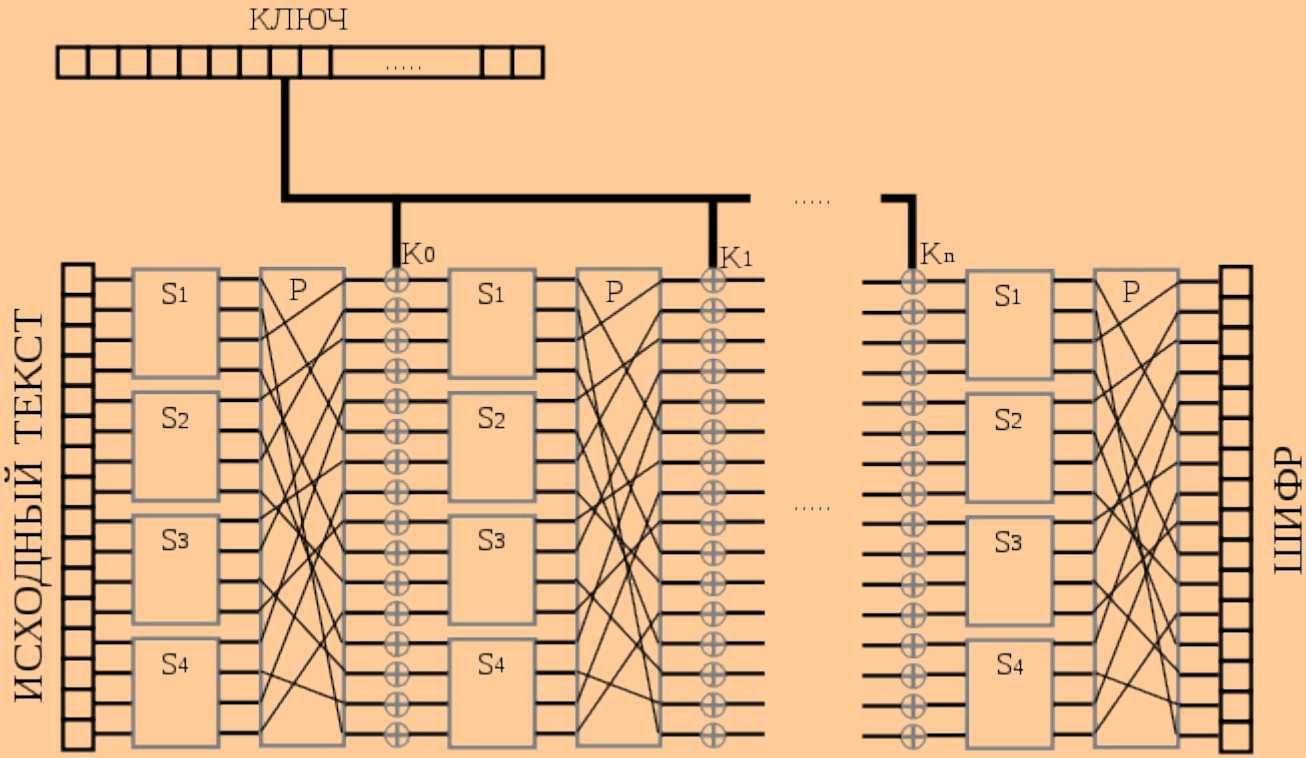
Симметричные криптоалгоритмы

Блочные шифры — SP-сети

S-блоки — подстановка (substitution) (даёт лавинный эффект)

P-блоки — перестановка (permutation) (распределение)

Примеры: AES, Serpent, SAFER



© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Сравнение блочных шифров

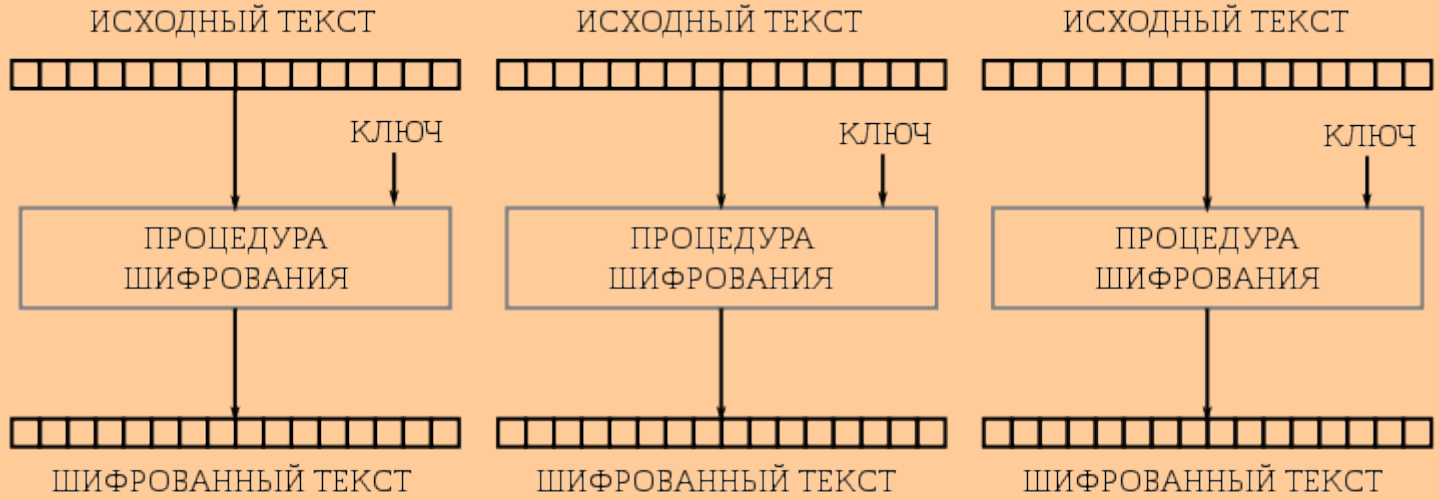
	Раундов	*Ключ (бит)*	*Блок (бит)*
DES (1977, США)	16	56	64
3DES (1978, США)	32/48	112/168	64
ГОСТ 28147-89 (1989)	32/16	256	64
IDEA (1991, ЕС)	8+1	128	64
CAST (1996, Канада)	12/16, 48	128,192,256	64, 128
Camellia (2000, Япония)	18/24	128,192,256	128
Blowfish (1993,Шнайер)	16	<448	64
Twofish (1998, Шнайер)	16	128,192,256	128
AES «Rijndael» (1998)	10-14	128,192,256	128
Serpent (1998)	32	128,192,256	128

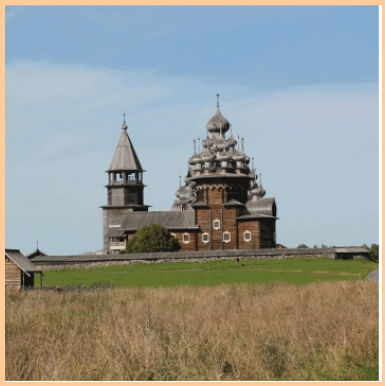
© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Режимы шифрования (методы применения блочных шифров)

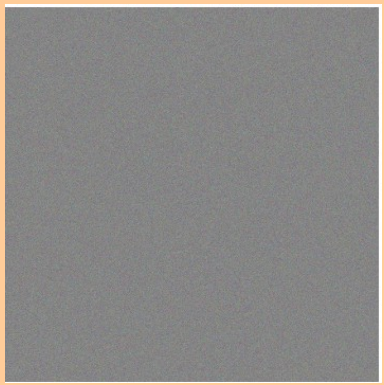
ECB (Electronic Codebook) — Режим электронной книги





Исходное изображение

Шифр в режиме ECB



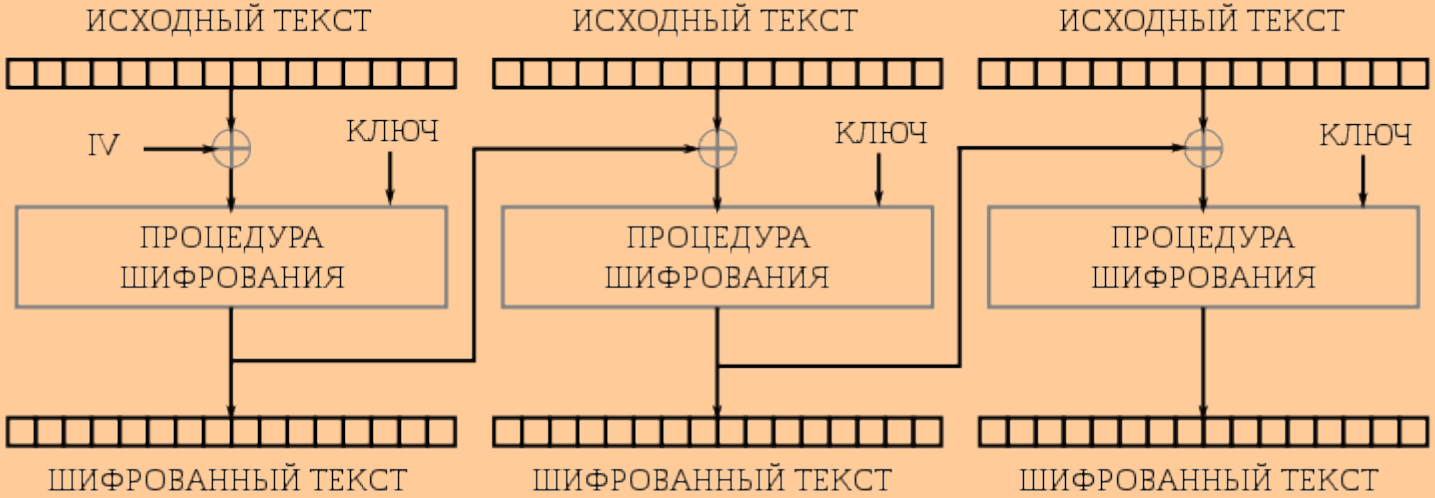
Шифр в др. режиме

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

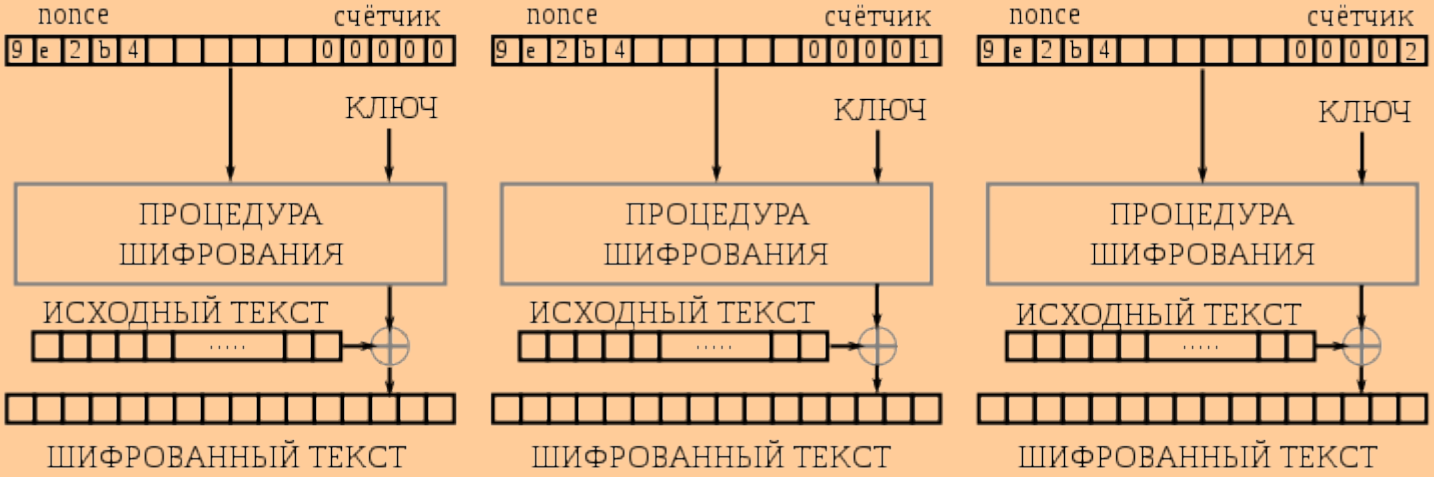
ВОПРОСЫ БЕЗОПАСНОСТИ

Режимы шифрования (методы применения блочных шифров)

CBC (Cipher Block Chaining) — Режим сцепления блоков шифротекста



CTR (CounTeR) — Режим счётчика



© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Криптографические хэш-функции

* *Необратимость*: для заданного значения хэш-функции m вычислительно неосуществимо найти блок данных X, для которого hash(X) = m.
* *Стойкость к коллизиям I рода*: для заданного сообщения M вычислительно неосуществимо подобрать другое сообщение N, для которого hash(M) = hash(N).
* *Стойкость к коллизиям II рода*: вычислительно неосуществимо подобрать пару сообщений (M, M'), имеющих одинаковый хэш.

Популярные хэш-функции:

MD5 (128 бит)
SHA-1 (160 бит) — на 25% медленнее MD5
SHA-2 (256/512 бит) — в 3 раза медленнее MD5
ГОСТ Р 34.11-94 (256 бит) — в 5 раз медленнее SHA-1
ГОСТ Р 34.11-2012 «Стрибог» (256/512 бит)

Поиск коллизий хэш-функций:

brute force ~ 2^n; birthday attack ~ $2^{n/2}$; MD5 ~ 2^{18}; SHA-1 ~ 2^{61}

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Имитовставка (Message Authentication Code — MAC)

K — ключ имитовставки (секретный) используется для предотвращения фальсификации сообщения

CBC-MAC — имитовставкой является последний блок шифротекста в режиме CBC

HMAC — на основе хэша (RFC 2104):

HMAC(*K*, *m*) = hash (((*K* ⊕ *opad*)||hash((*K* ⊕ *ipad*)||*m*))

opad = 0x5C 0x5C 0x5C …

ipad = 0x36 0x36 0x36 …

(предотвращение атаки length extension)

(урезание вывода хэша: hmac-md5-96 и т. п.)

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Электронная цифровая подпись (PKCS#1, RFC 3447)
(SSA — Signature Scheme with Appendix)

RSASSA-PKCS1-v1_5 (детерминированная схема)

M — исходное сообщение ($M<n_{RSA}$), *AID* — идентификатор алгоритма

$H = \text{hash}(M) \rightarrow T = \text{DER}(AID||H) \rightarrow$

$EM = 0x00||0x01||0xFF...0xFF||0x00||T$ (длина *EM* соотв. длине n_{RSA})

$ЭЦП = \text{RSA}(K_{pri}, EM)$

AID: md5WithRSAEncryption, sha1WithRSAEncryption, sha256WithRSAEncryption
DER (Distinguished Encoding Rules) — ITU-T X.690 (ISO/IEC 8825-1)

RSASSA-PSS (вероятностная схема)

При одинаковых входных данных получаются разные подписи, т. к. используется salt.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Public Key Infrastructure (PKI) — Инфраструктура открытых ключей

1. Закрытый ключ известен только владельцу.
2. Окрытый ключ + информация о владельце = сертификат.
Сертификат имеет ЭЦП, сформированную третьей стороной.
3. Пользователи ключей не доверяют друг другу. Выбираются субъекты, подписям которых пользователи доверяют.

Интернет-PKI (или X.509 PKI): удостоверяющие центры (certification authority).

Web-of-trust (сеть доверия) — PGP: любой участник подписывает, пользователь сам выбирает, кому доверять.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Сертификаты ITU-T X.509 (ISO/IEC 9594-8, RFC 5280)

Abstract Syntax Notation One (ASN.1)

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 25 (0x19)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: C=RU, ST=Karelia, L=Petrozavodsk, O=PetrSU, OU=Lab127 Team, CN=thermo.karelia.ru
  Validity
    Not Before: Jul 24 08:36:35 2010 GMT
    Not After : Jul 21 08:36:35 2020 GMT
  Subject: C=RU, ST=Karelia, L=Petrozavodsk, O=PetrSU, OU=DIMS&PhE, CN=kompot.petrsu.ru
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (1024 bit)
    Modulus: 00:bf:3e:8e:f2:92:e9:e9:1e:79:6e:b1:58:58:3b:...
    Exponent: 65537 (0x10001)
  X509v3 extensions:
     ...
  Signature Algorithm: sha1WithRSAEncryption
    99:3e:56:9b:7d:b9:a9:a1:9e:c0:2d:f4:ea:e3:8a:de:29:13:...
```

DER (*.der) или DER в BASE64 (*.pem, *.cer, *.crt)

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Правила проверки PKI

1. Проверить ЭЦП предоставленного сертификата (при помощи открытого ключа удостоверяющего центра).

2. Проверить, что сертификат не отозван.

3. Проверить срок действия сертификата.

4. Проверить, что другая сторона соответствует имени субъекта сертификата.

5. Проверить аутентичность другой стороны — другая сторона предоставляет ЭЦП некоторого (заранее обговорённого сообщения), сформированную при помощи своего закрытого ключа. ЭЦП проверяется открытым ключом из сертификата.

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014

ВОПРОСЫ БЕЗОПАСНОСТИ

Отзыв сертификатов X.509

Certificate Revocation List (CRL) — список отозванных сертификатов — текстовый файл с ЭЦП удостоверяющего центра (распространяется через публичные сервисы)

Online Certificate Status Protocol (OCSP), RFC 6960

TLS Extension — Certificate Status Request (OCSP Stapling), RFC 6066 — TLS-сервис во время фазы согласования предоставляет OCSP-токен, подтверждающий, что сертификат не отозван

Популярные удостоверяющие центры:
Verisign, Thawte /Symantec/ (www.verisign.com, www.thawte.com),
GlobalSign (www.globalsign.com),
Comodo (www.comodo.com)

© Петрозаводский госуниверситет, А. В. Соловьев, 2006-2014