if(is) internet security.

Institute for Internet Security (Germany)

# Методы шифрования

http://www.if-is.net/crypto-poster/

Дата: 2014-05-26
Автор: Dominique Petersen
petersen@internet-sicherheit.de
Графика: David Bothe
bothe@internet-sicherheit.de

## Симметричное шифрование

В симметричных криптосистемах для шифрования и расшифрования используется один и тот же ключ. Ключ выбирается заранее и известен только обеим сторонам коммуникационного канала, Сохранение ключа в секретности является важной задачей для установления и поддержки защищенного канала связи. Из за высокой скорости работы симметричного шифрования его хорошо использовать при шифровании большого количества данных на жёстких дисках или в файловых контейнерах. Потоковый шифр RC4 например, может быть полностью взломан и расшифрован службой АНБ в реальном времени, поэтому лучше использовать алгоритмы Cammellia или AES с размером ключа в 128 бит и выше.

максимально не надежный
ненадёжный
средней надежности
надежный
наиболее надежный
максимально надежный

RC4
DES
Triple-DES
Camellia 128
AES 128
Camellia 192
AES 192
Camellia 256
AES 256

## Асимметричное шифрование

В системах с открытым ключом используются два ключа - открытый (PublicKey) и закрытый (PrivateKey) связанные математически друг с другом. С помощью их и происходит шифрование и дешифрование данных. Открытым ключом данные зашифровываются и только с помощью закрытого ключа их можно снова расшифровать. Закрытый ключ так же используется для генерации ЭЦП. Асимметричное шифрование используется для шифрования электронной почты и в интернете (HTTPS, Верификация цифровой подписи), а так же для идентификации людей (nPA-German identity card) и компьютеров. При ассиметричном шифровании лучше использовать алгоритмы RSA или ECC с размерами ключей 2048 и 192 бит и выше.Так как некоторые варианты эллиптических кривых NIST были манипулированы службой АНБ, то стоит проверить использование этого алгоритма вообще.

DSA
(signing only)
RSA 1024
RSA 2048
RSA 4096
ECC 192
(elliptic curves NIST)
ECC 224
(elliptic curves NIST)
ECC 256
(elliptic curves NIST)
ECC 384
(elliptic curves NIST)
ECC 521
(elliptic curves NIST)
RSA 8192

## Криптографическая хеш-функция

Хеш-функция сжимает входной поток данных в одно число определённой длины (так называемый Fingerprint ,например 160 бит). Так как асимметричное шифрование очень медленное и использование его для большого количества данных не приводит к желаемому результату, хеш-функция обретает большое значение в шифровании данных . При шифровании этого числа (Fingerprint) закрытым ключом (PrivateKey) получатель может проверить, пришло ли сообщение от отправителя или же сообщение было в сети кем то манипулировано. Если при шифровании данных использовать уже взломанный MD5 метод шифрования, то при этом не составляет ни какой проблемы заменить любое настоящие сообщение на манипулированное. Поэтому рекомендуется использовать методы шифрования из семьи RIPE-MD и SHA2/3 с размерами ключей 256 бит и выше.

MD5
RIPE-MD 160
SHA1
SHA3 224
SHA2 224
RIPE-MD 256
SHA3 256
SHA2 256
RIPE-MD 320
SHA3 384
SHA2 384
SHA3 512
SHA2 512