«Понятия шифрования сообщений, электронной-цифровой подписи и авторизации в сервисах Internet»

Internet - ***Inter***connected ***Net***works — объединённые сети.

Примеры сервисов Internet:

World Wide Web – сервис, через Internet обеспечивающий доступ к информации. Самый распространенный сегодня сервис.

E-mail - Электронная почта.

FTP - передача файлов.

Grid - доступ к вычислительным мощностям и ресурсам хранения данных

IP-телефония

Видео-конференции

. . .

Сцитала - шифр перестановки

Сцитала использовалась в войне Спарты против Афин в конце V века до н.э. спартанским полководцем Лисандром.

Сцитала представляла собой жезл, на который наматывалась лента из пергамента. На ленту наносился текст вдоль оси сциталы, так, что после разматывания текст становился нечитаемым. Для его восстановления требовалась сцитала такого же диаметра.

Зашифрованная информация — лента с непонятным текстом
Ключ — сцитала
Алгоритм — способ намотки ленты на сциталу

Гай Юлий Цезарь — Метод сдвига

Юлий Цезарь не доверял гонцам. Поэтому, отправляя письма своим генералам, он заменял каждую букву A в своём сообщении на D, каждую B на E, и т.д. То есть сдвигал алфавит на 3 буквы.

Только тот, кто знал правило «сдвига на 3» мог расшифровать его послание в I веке до н.э

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Dyh Fdhvdu! Prulwxul wh vdoxwdqw!
Ave Caesar! Morituri te salutant!

Зашифрованная информация — лист с непонятным текстом
Ключ — пергамент с прямым и сдвинутым алфавитом.
Алгоритм — заменить одну букву на другую.

Метод симметричного шифрования.

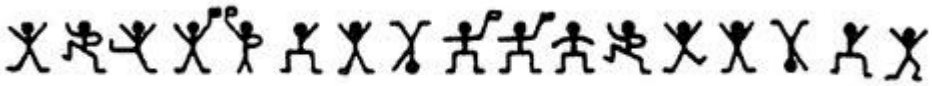
Все исторически известные ручные методы шифрования были симметричными. Другими словами при шифровании и расшифровке использовались одинаковые физические ключи + алгоритм.

Абонент А

Информация +
Метод шифрования =
Зашифрованная информация

Абонент В

Зашифрованная информация
+ (-)Метод шифрования=
Информация



→ → Зашифрованная информация → →

Симметричная схема шифрования широко используется в сервисах Интернет.

Простейший пример - пароль для доступа куда-либо.

Глобальная проблема симметричных шифров состоит в сложности управления ключами:

Как доставить ключ получателю без риска, что его перехватят?

Злоумышленник, имеющий ключ, может читать, изменять и подделывать любую информацию, зашифрованную или заверенную этим ключом.

Метод Асимметричного шифрования.

В 20 веке разрабатываются математические схемы, которые позволяют создать такую неодинаковую пару ключей, что:

- то, что зашифровано с помощью *одного* ключа можно расшифровать, только имея *другой* ключ, и наоборот;
- один ключ (***секретный***, ***закрытый***, private key) содержит в себе другой ключ (*открытый*, public key);
- Хотя ключевая пара математически связана, вычисление ***закрытого*** ключа из *открытого* в практическом плане *сегодня* невыполнимо.

Таким образом появляется **Криптография с открытым ключом**.

Открытый ключ известен всем, ***закрытый*** держится владельцем в строгой тайне.

Примеры криптосистем с открытым ключом:

Diffie-Hellman - 1976, названа в честь её создателей;

RSA - 1977, тоже названа в честь ее изобретателей: Рона Ривеста, Ади Шамира и Леонарда Адлмана);

Elgamal - 1984, автор Тахир Эльгамаль;

ACE Encrypt - научно-исследовательская лаборатория IBM, Швейцария, Цюрих;

PSEC-KEM - Nippon Telegraph and Telephone Corp., Япония;

RSA-KEM - проект ISO/IEC 18033-2

ГОСТ Р 34.10-2001 - усовершенствованный алгоритм ГОСТ Р 34.10-94

Для эффективного использования открытых ключей создана Инфраструктура открытых ключей (**PKI** - Public Key Infrastructure)

Это комплексная система, которая связывает открытые ключи с личностью пользователя посредством Удостоверяющего Центра.

1. ***Закрытый*** ключ известен только его владельцу, *открытый* ключ известен всем;
2. Удостоверяющий Центр создает сертификат *открытого* ключа, таким образом удостоверяя владельца закрытого ключа;
3. Никто не доверяет друг другу, но все доверяют Удостоверяющему Центру;
4. Удостоверяющий Центр подтверждает или опровергает то, что лицо, поименованное в сертификате, владеет ***секретным*** ключом, который соответствует этому открытому ключу.

Шифрование сообщений

1. Сторона А хочет зашифровать документ *открытым* ключом стороны В.

2. Чтобы убедиться, что *открытый* ключ действительно принадлежит стороне В, сторона А запрашивает сертификат открытого ключа стороны В у Удостоверяющего Центра.

3. Сторона А зашифровывает документ полученным от Удостоверяющего Центра *открытым* ключом стороны В.

4. Только сторона В может расшифровать сообщение, так как владеет соответствующим ***закрытым*** ключом.

Сторона А свое собственное зашифрованное сообщение расшифровать не может.

Электронно-цифровая подпись (ЭЦП)

1. Сторона А формирует ЭЦП документа ***закрытым*** ключом и отправляет документ стороне Б.

2. Сторона Б запрашивает сертификат *открытого* ключа стороны А у удостоверяющего центра, а также информацию о действительности сертификата.

3. Если сертификат стороны А действителен и проверка ЭЦП прошла успешно, значит документ был подписан стороной А, а не кем-то другим.

4. Правильность цифровой подписи подтверждает и то, что документ не изменялся.

Таким образом, цифровая подпись является средством ***аутентификации*** и ***контроля целостности данных***.

Авторизация

Сертификаты могут использоваться для подтверждения личности пользователя и задания полномочий, которыми он наделен. Например, право просматривать информацию или разрешение вносить изменения в материал, представленный на web-сервере (http://cic.gridops.org/index.php?section=home&page=gettingstarted).

Сервисы аутентификации, авторизации и учета имеют ключевое значение для любой распределенной инфраструктуры для высокопроизводительных вычислений (HPC) и позволяют:

- надежно определить серверы и пользователей (аутентификация);
- обеспечить политики доступа для пользователей и серверов (авторизация);
- получить информацию об использовании ресурсов, и управлять системой доступа, связанной с системой учета.

Проблемы, которые могут возникнуть при использовании Инфраструктуры открытых ключей.

- *Закрытый* ключ защищается *парольной фразой* – более длинным, сложным и, теоретически, более надёжным вариантом пароля. Забыли фразу — придется менять ключевую пару.
- Цифровая подпись несёт принцип *неотречения*, который означает, что отправитель не может отказаться от факта своего авторства информации подписанной его цифровой подписью.
- Цифровая подпись, в отличие от собственноручной, свидетельствует не о том, что конкретный индивидуум (физическое лицо) заверил информацию, а что конкретный *криптографический ключ* заверил информацию.