**Подготовил :КОНЕ Сирики НФИБд-01-20**

**Операционные системы: Доклад**

*Методы криптования на основе открытого ключа(Шифрование с открытым ключом)*

**Содержание**

* Симметричный шифр
* Ассиметричный шифр
* Виды ассиметричных шифров
* Пример
* Заключение
* Список литературы

**Симметричный шифр**

**Симметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи совпадают.**

*Стороны, обменивающиеся зашифрованными данными, должны знать* ***общий секретный ключ.***

Симметричный шифр

Симметричный шифр

**Достоинства:**

Всего один зашифровывающий / расшифровывающий ключ

**Недостатки:**

Процесс обмена информацией о секретном ключе представляет собой брешь в безопасности.

Для передачи секретного ключа необходим закрытый канал связи.

**Ассиметричный шифр**

**Ассимметричный шифр** – метод передачи шифрованной информации, в котором зашифровывающий и расшифровывающий **ключи не совпадают.**

***Ассиметричное шифрование является односторонним процессом****.*

*Данные шифруются только открытым ключом*

*Расшифровываются только секретным*

*Открытый и секретный ключ связаны между собой.*

Ассиметричный шифр

Ассиметричный шифр

**Достоинства:**

Для передачи ключа не нужен закрытый канал связи.

Открытый ключ может быть свободно распространен, это позволяет принимать данные от всех пользователей.

**Недостатки:**

Ресурсоемкий алгоритм шифрования / дешифрирования

**Виды ассиметричных шифров**

**RSA**

Rivest-Shamir-Adleman (Ривест-Шамир-Адлеман)

**DSA**

Digital Signature Algorithm (Алгоритм цифровой подписи)

**EGSA**

El-Gamal Signature Algorithm (Алгоритм ЭЦП Эль-Гамаля)

**ECC**

Elliptic Curve Cryptography (Криптография эллиптической кривой)

**ГОСТ Р 34.10-94**

Российский стандарт схожий с DSA

**ГОСТ Р 34.10-2001**

Российский стандарт схожий с ECC

**Пример шифрование RSA**

**Шифрование**

Формула для шифрования:



Возьмем к примеру сообщение



Запишем его кодом в соответствии с алфавитом



Результат:



Пример:

 

**Пример дешифрование**

**Дешифрирование**

Формула для дешифрирования



Шифрованное сообщение



Результат:



В соответствии с алфавитом:



Пример:



 

**Заключение**

Как симметричное, так и асимметричное шифрование играет важную роль в обеспечении безопасности конфиденциальной информации и коммуникации в современном цифровом мире. Оба шифра могут быть полезны, ведь у каждого из них есть свои преимущества и недостатки, поэтому они применяются в разных случаях.

Поскольку криптография как наука продолжает развиваться для защиты от более новых и более серьезных угроз, симметричные и асимметричные криптографические системы всегда будут иметь отношение к компьютерной безопасности.

**Список литературы**

Венбо Мао Современная криптография. Теория и практика. — М.: Вильямс, 2005. — 768 с.

Коутинхо С. Введение в теорию чисел. Алгоритм RSA. — М.: Постмаркет, 2001. — 328 стр.

Фергюсон Н., Шнайер Б. Практическая криптография — М.: «Диалектика», 2004. — 432 с.

Википедия [Электронный ресурс] – Режим доступа: [http://ru.wikipedia.org](http://ru.wikipedia.org/)