**СИММЕТРИЧНАЯ КРИПТОГРАФИЯ**

*В лекции*

-         *Суть симметричного шифрования*

-         *Классификация симметричных криптосистем*

-         *Блочные и потоковые шифры*

-         *Алгоритм DEA*

-         *Алгоритм TDEA*

-         *Стандарт шифрования AES*

-         *Алгоритм IDEA*

-         *Другие симметричные криптоалгоритмы*

-         *Шифры Брюса Шнайера и шифры Ривеста  
Несколько слов о безопасности симметричных криптосистем*

В настоящее время все существующие криптосистемы принято разделять на два класса: симметричные и асимметричные.

Соответственно, говорят о симметричной криптографии и асимметричной криптографии.

**В симметричных криптосистемах** одним и тем же секретным ключом осуществляется и шифрование, и расшифрование:

*Ek(P) = C*

*Dk(C) = P,*

где *Е* – функция зашифрования, *k* – ключ, *P* – открытый текст, *С* – шифртекст,   
*D* – функция расшифрования.

При этом справедливо следующее равенство:

*Dk(Ek(P)) = P*

**Потоковые и блочные шифры**

Алгоритмы, которые обрабатывают открытый текст побитово (побайтово), называют ***потоковыми алгоритмами*** или потоковыми шифрами.

Алгоритмы, которые обрабатывают группы битов (блоки) открытого текста, называют ***блочными алгоритмами*** или блочными шифрами.

Долгое время в компьютерных алгоритмах типичный размер блока был равен 64 битам. Это достаточно большое значение, чтобы затруднить анализ, и в то же время достаточно малое, чтобы быть удобным для работы.

В настоящее время используются 128-разрядные блоки, так как длина блока в 64 бита не удовлетворяет современным требованиям эффективности и надежности алгоритмов.

Наиболее широко применяемыми на практике симметричными криптосистемами долгое время являлись системы DES (стандарт США), IDEA (европейский стандарт), ГОСТ (стандарт РФ) и их модификации.

**Алгоритм DEA**

Самым известным и широко распространенным компьютерным алгоритмом шифрования является **алгоритм DEА**, лежащий в основе DES (Data Encrypt Standard) - стандарта шифрования данных США.

Алгоритм DEA был опубликован в 1973 году и в течение почти 20 лет считался криптографически стойким.

В процессе шифрования с помощью алгоритма DEА последовательно производятся преобразования (раунды) над 64-битовыми блоками:

*P, Ф1, Ф2, ..., Ф16, P-1*,                                                     (1.1)

где *P* – заданная подстановка; *Фi**= ViT*  - преобразование (сеть) Файстеля  
(H. Feistel ), являющееся основой многих симметричных алгоритмов: 

*T (* *L, R) = ( R, L) –*перестановка левой и правой частей;

*Vi = V(Li, Ri) = (Li, Ri ⊕ F(Ri-1, Ki))*;

*L0R0;    Li= Ri-1,      Ri = Li-1⊕ F(Ri-1, Ki),   (i = 1,...,16);*

где *Ki*– ключи, получаемые на основе 56-битового секретного ключа*K;  
F –*функция раунда.

Схему формирования шифра DEA см. в презентации к лекции.

Расшифрование производится с помощью преобразований (1.1) на основе ключа *K*, причем ключи *Ki* генерируются в обратном порядке.

Обратим внимание, оригинальный алгоритм DEA был разработан для реализации в виде микросхемы, а не эффективного программного кода, поэтому на практике оказывается очень медленным.

**Алгоритм TDEA**

Одной из составляющих стандарта шифрования данных США 1999 г. является **алгоритм TDEA («тройной» DEA**). В алгоритме TDEA для зашифрования используется три ключа и трижды применяется алгоритм DEA:

*C = Ek3(Dk2(Ek1(P)))*

Расшифрование представляет собой следующее преобразование:

*P = Dk1(Ek2(Dk3(C)))*

Длина ключа TDEA оказывается равной 168 бит.

            В [Federal Information Processing Standard PUB 46-3] содержатся следующие рекомендации относительно TDEA.

* Использование оригинального алгоритма DEA с 56-битовым ключом допускается только в действующих системах. Новые разработки должны поддерживать TDEA.
* Правительственным организациям, применяющим системы на основе DEA, настоятельно рекомендуется перейти к использованию TDEA.

Однако существенным недостатком TDEA является то, что алгоритм оказывается очень медленным в условиях программной реализации. Оригинальный алгоритм DEA был разработан в середине 70-х годов XX в. для реализации в виде микросхемы, а не эффективного программного кода. Алгоритм TDEA, соответственно, оказывается еще более медленным. Кроме того, длина блока (64 бит), используемая в DEA и TDEA, не удовлетворяет современным требованиям эффективности и защищенности, предпочтительнее использование блоков большей длины.

**Стандарт шифрования AES**

Названные проблемы призван был решить новый усовершенствованный стандарт шифрования AES (Advanced Encryption Standard). С 1997 г. NIST (Национальный институт стандартов и технологий США) принимал предложения по созданию такого стандарта. Обратим внимание на требования, которые предъявлялись  NIST: AES должен иметь стойкость не меньше TDEA, но быть существенно эффективным, кроме того, AES должен быть симметричным блочным шифром с длиной блока в 128 бит, поддерживающим использование 128-, 192- и 256-битовых ключей.

В течение нескольких лет криптографическое сообщество разрабатывало и обсуждало приемника для алгоритма DES. В результате был создан алгоритм **AES** (Advanced Encryption Standard), который был опубликован в 2001 году (FIPS 197).

Новый стандарт был принят на основе открытого конкурса, в котором участвовали алгоритмы, предложенные математиками из многих стран мира: США, Канады, Австралии, Бельгии, Германии, Норвегии, Франции, Японии, Южной Кореи, Коста-Рики. Победителем конкурса стал алгоритм Rijndael, разработанный бельгийскими криптографами Винсентом Рэменом и Йоном Даменом. Название алгоритма образовано из первых букв фамилий его авторов, поэтому в транскрипции с фламандского оно произносится примерно так: «рэндал». [Голдовский, 85]

AES представляет собой блочный, симметричный алгоритм шифрования с длиной блока 128 бит. Длина ключа может принимать значения 128, 192 или 256 бит (AES-128, AES-192 и AES-256, соответственно). Таким образом, в обозримом будущем алгоритм защищен от атак методом полного перебора ключей. К достоинствам алгоритма относятся также высокое быстродействие и умеренные требования к памяти. И, следовательно, он может быть реализован в различных устройствах, включая SIM-карты  мобильного телефона и смарт-карты.

Обратим особое внимание и на то, что алгоритм   Rijndael не защищен патентами и доступен для свободного использования в любых программных продуктах. Поэтому, AES стал практически (де-факто, не де-юро) международным стандартом.

**Алгоритм IDEA**

Тщательному анализу со стороны криптоаналитиков подвергался широко известный **алгоритм IDEA**, представляющий собой симметричный блочный шифр с длиной ключа 128 бит.

В процессе преобразования IDEA данные подвергаются комбинированным операциям XOR, побитовому сложению и умножению в течение 8 раундов. В результате получаются сложные преобразования, вызывающие трудности криптоанализа.

Алгоритм IDEA был разработан сотрудниками Швейцарского федерального института технологий (г. Цюрих) Сюдзя Лай и Джеймсом Мэсси. Опубликован в 1990/1991 годах.

Он считается более стойким, чем традиционный DEA, и представляет основу программы шифрования PGP, применяемой пользователями Internet.

Разработчиком программы PGP, вначале известной как программы шифрования электронной почты, является Фил Циммерман. Создав PGP, он опубликовал  программу в Internet. За это власти США возбудили против него уголовное дело.  «За экспорт криптостойких шифров» его приравняли к торговцам оружием и наркотиками, признав тем самым, что алгоритмы, входящие в PGP - IDEA и RSA «оказались слишком крепким орешком для правительственных чиновников».

Благодаря действительно «хорошим» алгоритмам шифрования и такой рекламе программа PGP быстро завоевала популярность у пользователей всего мира. После закрытия уголовного дела Ф. Циммерман основал фирму PGP Inc. Сегодня он консультирует крупнейшие компании и организации по вопросам безопасности и является признанным специалистом в области криптографии.

**Другие симметричные криптоалгоритмы**

Таким образом, существует множество симметричных криптоалгоритмов. Отметим следующие из них:

**алгоритм ГОСТ** с 256-битовым ключом, основанный на концепции алгоритма DEA, но более оптимальный для программной реализации;

**алгоритм Blowfish** с переменной (до 448 бит) длиной ключа, разработанный Б. Шнайером (B. Schneier) в 1993 г.;

**алгоритм RC5**, разработанный Р. Райвестом (R. Rivest) в 1995 г. и  представляющий собой блочный шифр с параметрами: размер блока, размер ключа, число раундов;

**алгоритм CAST-128**, разработанный в 1997 г. К. Адамсом (C. Adams) и С. Таваресом (S.Tavares), который подвержен криптоанализу только полным перебором ключей (допускается использование ключей длиной от 40 до 128 бит);

Особо отметим алгоритмы, разработанные двумя известными специалистами в области криптографии - Брюсом Шнайером и Роном Райвестом.

**Шифры Брюса Шнайера и шифры Ривеста**

**Брюс Шнаейр (B. Schneier)**  -  независимый консультант и самый известный во всем мире специалист по криптографии

**Алгоритм Blowfish** (1993 г.) – 64 разрядный блочный шифр с переменной (от 32 до 448 бит) длиной ключа

Превосходит DES по скорости и стойкости. НЕПАТЕНТОВАННЫЙ, бесплатный и беспошлинный. Используется во многих коммерческих приложениях.

**Алгоритм Twofish** (кандидат на роль AES) – 128-разрядный блочный алгоритм, поддерживающий ключи длиной 128, 192, 256 разрядов.

Разработан компанией Б.Шнайера Counterpane Systems. НЕПАТЕНТОВАННЫЙ, бесплатный и беспошлинный.

**Ronald (Ron) Rivest** – ключевая фигура в современной криптографии. Он - профессор Массачусетского технологического института, основатель компании RSA. Изобрел целую серию шифров, которые носят его имя – **Ron’s code.**

Заметим, что в отличие от шифров Б. Шнаейреа, все шифры Ривеста -

ПАТЕНТОВАННЫЕ

**RC2 –**64-разрядный блочный шифр с ключом переменной длины (экспорт при ограничении ключа до 40 разрядов). Скорость больше, чем у DES.

**RC4** (1994 г.) – усовершенствованный RC2.

**RC5** (1995г.) – усовершенствованный RC4. Семейство алгоритмов, так как реализуется для различных параметров: длина блока, длина ключа, количество раундов.

**RC6**(кандидат на роль AES) – 128-блочный шифр на базе RC5**.**

**Несколько слов о безопасности симметричных криптосистем**

Забегая вперед, обратим внимание, что для криптоанализа симметричных систем разработано множество методов:

-         метод полного перебора ключей,

-         методы криптоанализа с использованием теории статистических решений,

-         разностный криптоанализ и его модификации,

-         линейный криптоанализ.

С помощью данных методов осуществлены эффективные криптоатаки на большинство симметричных криптосистем.

Безопасность симметричных криптосистем определяется двумя факторами:

-         стойкостью самого алгоритма,

-     длиной ключей.

Критерием качественного шифрования служит следующий принцип:

**стойкость шифра должна определяться только секретностью ключа**(правило Кирхгоффса -Dutchman A. Kerckhoffs) .