Криптоанализ блочных шифров

Дмитрий Ширяев

СПбГУ, 2005 г.

Эпиграф

- Существует только один путь стать хорошим разработчиком криптографических алгоритмов --- быть хорошим криптоаналитиком и взламывать алгоритмы. Множество. Снова и снова. Только после того, как обучающийся продемонстрирует способности к криптоанализу чужих алгоритмов, он сможет серьезно браться за разработку собственных алгоритмов.

Брюс Шнайер (Bruce Schneier)

План

- Часть 1: Блочные шифры
- Часть 2: Криптоанализ
- Часть 3: Различные атаки

- Выводы
- Источники дополнительных сведений

Часть 1: Блочные шифры

- Симметричная криптосистема
- Блочные криптосистемы разбивают текст сообщения на отдельные блоки и затем осуществляют преобразование этих блоков с использованием ключа.

Преобразование должно использовать следующие принципы:

- Рассеивание (diffusion) - т.е изменение любого знака открытого текста или ключа влияет на большое число знаков шифротекста, что скрывает статистические свойства открытого текста;
- Перемешивание (confusion) - использование преобразований, затрудняющих получение статистических зависимостей между шифротектстом и открытым текстом.

Параметры блочного шифра

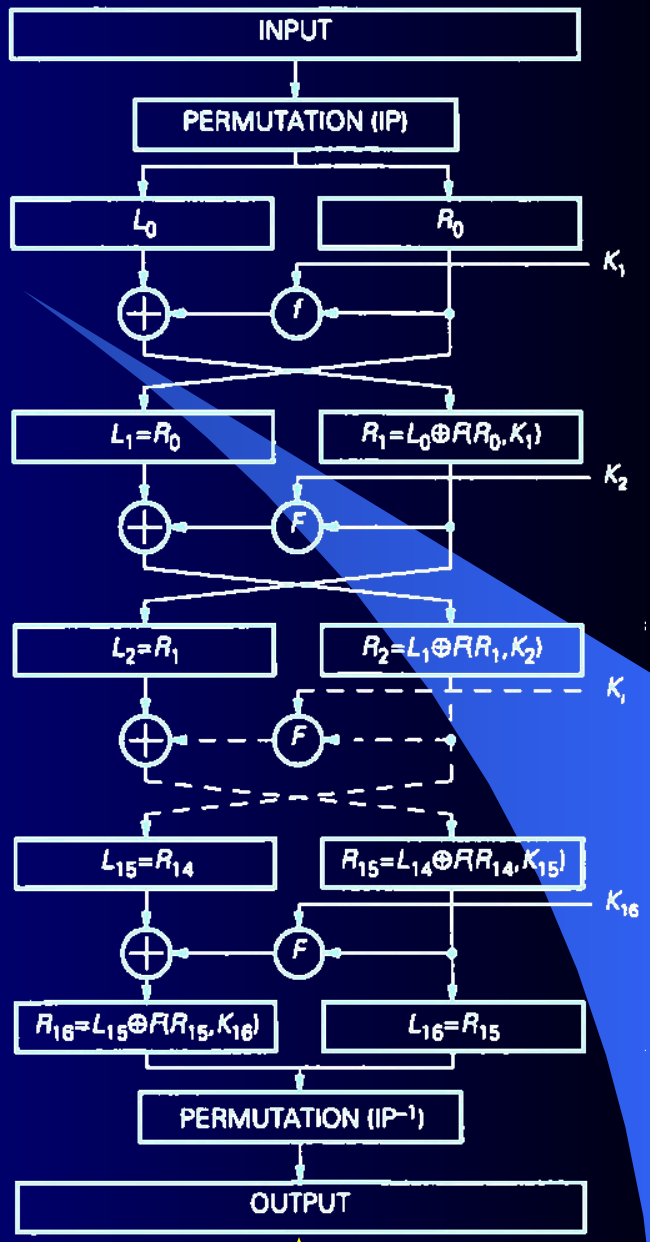
- Числовые параметры алгоритма:
  - размер шифруемого блока данных
  - размер ключа
  - размер “шагового” ключа
  - число раундов шифрования
- Функция шифрования
- Набор функций для выработки шаговых ключей
- Фиксированные перестановки

Алгоритм DES

Data Encryption Standard

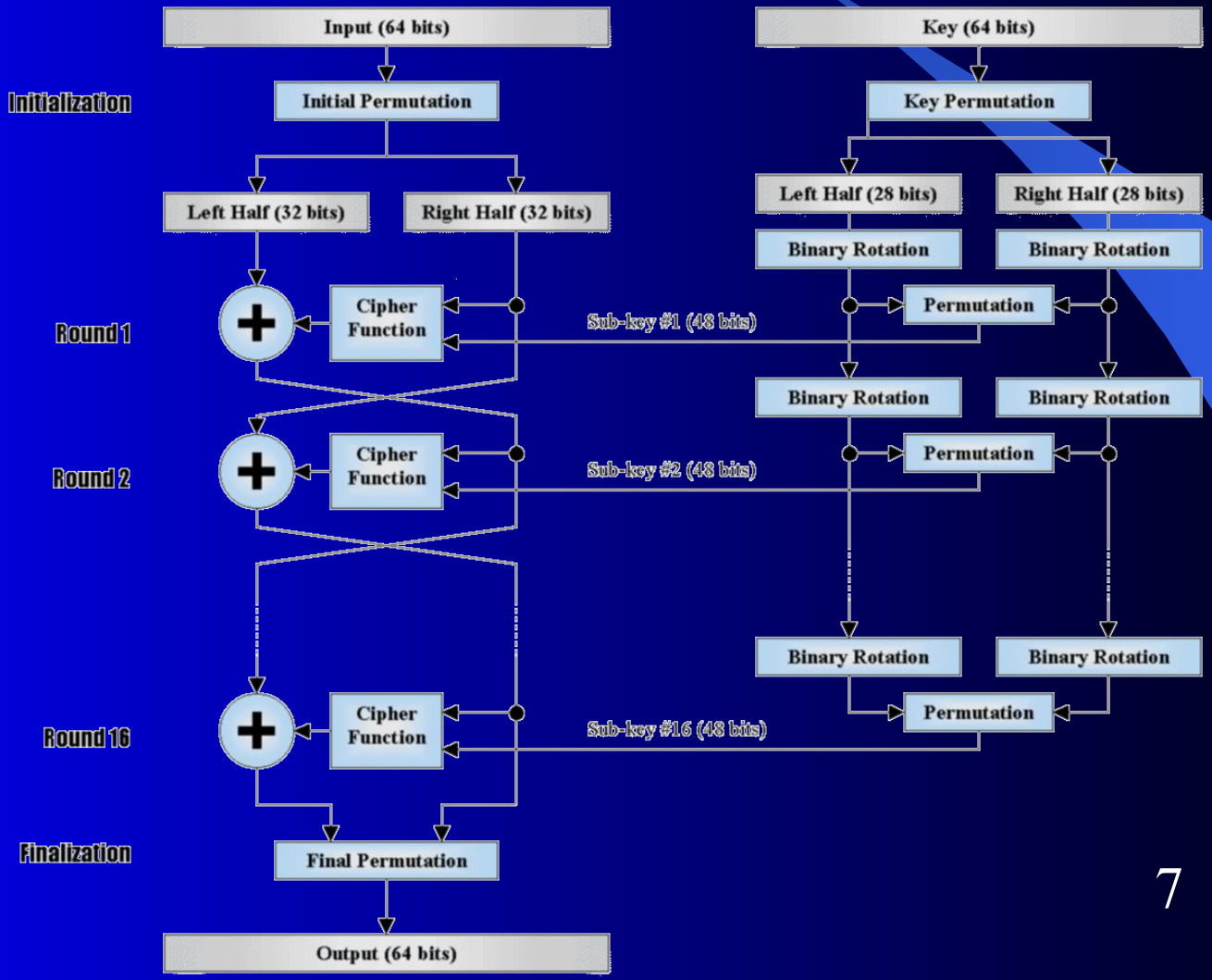
Американский
стандарт шифрования
на протяжении 1974-2000 г.г.

Длина блока 64 бит
Длина ключа 56 бит
Размер ключегого элемента 48 бит
Число раундов 16



Сеть Файстеля

Алгоритм DES: более подробно



Блоки подстановки (S-boxes)

- S-boxes созданы для того, чтобы запутать зависимость между текстом и шифротекстом
- В DES S-boxes с помощью фиксированных таблиц преобразуют 6-битовый вход в 4-битовый выход, соответственно 48 бит преобразуются в 32
- В ГОСТ используются переменные S-boxes

DES S-boxes ⟶

row	column number															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1																
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2																
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3																
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4																
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5																
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6																
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7																
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8																
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 7.8: DES S-boxes.

Часть 2: Криптоанализ

- Вопрос: Что же такое криптоанализ?

Криптоанализ – это отрасль знаний, целью которой является поиск и исследование методов взлома криптографических алгоритмов, а также сама процедура взлома.

Часть 2: Криптоанализ
Различные типы

- Ciphertext Only – анализ на основе только шифротекста
- Known Plaintext – анализ на основе невыбранного открытого текста
- Chosen Plaintext – анализ на основе выбранного открытого текста
- Chosen Ciphertext – анализ на основе выбранного шифротекста

Часть 2: Криптоанализ
На практике

Реальный криптоанализ основан на трех вещах:

- Изучение системы шифрования в целом
- Изучение особенностей исходного текста
- Изучение особенностей ключевой системы

Свойство дополнительности (Complementation property)

- Взаимосвязь между парами текст-шифротекст при обращении текста и ключа
- Например, в DES:

Если $C = DES(P, K)$ то $\overline{C} = DES(\overline{P}, \overline{K})$

Часть 2: Криптоанализ
Восстановление ключа

- Brutal-Force Attack – атака методом “грубой силы”, т.е. полным перебором ключей
- Основная цель любого метода криптоанализа – улучшить время Brutal-Force Attack, или улучшить имеющееся соотношение время/память
- Key-recovery – метод нахождения наиболее вероятного раундового ключа, с помощью перебора различных исходных текстов. Используется в большинстве методов криптоанализа

Часть 3: Различные атаки

- Дифференциальный криптоанализ
- Линейный криптоанализ
- Модификации дифференциального и линейного анализов
- Интерполяционный криптоанализ
- Методы, основанные на слабости ключевых разверток

Дифференциальный анализ: История

- Разработан в 1990 году израильскими криптографами Эли Бихамом (Eli Biham) и Али Шамиром (Ali Shamir)

Эли Бихам

Али Шамир

Дифференциальный анализ: Основные идеи

- Chosen-plaintext метод
- Выбираем пары входных текстов с фиксированной разностью, смотрим, как отличаются шифры от них
  $\Delta X = X_1 \oplus X_2 \quad \Delta Y = Y_1 \oplus Y_2$
- Анализируя много таких пар, находим наиболее вероятный ключ

Дифференциальный анализ: Более подробно

- Пусть в алгоритме есть S-box с n-битовым входом и m-битовым выходом
- Дифференциал – это пара: разность входных данных и разность выходных данных нашего преобразования
- Если Q - это количество различных пар входов, дающих этот дифференциал, то $p=Q/2^n$ – вероятность этого дифференциала
- Дифференциальная характеристика – это последовательность разностей после каждого раунда

$$\Delta X \xrightarrow{P} \Delta Y$$

$$(\Delta_0; \Delta_1; \ldots; \Delta_R)$$

- Построив дифференциальную характеристику на раундах с 1го по предпоследний, проводим Key-recovery атаку на последнем раунде.

- Для взлома DES необходимо 2^{47} выбираемых нами входных текстов
- Защита – минимизировать максимальные вероятности p, максимизировать количество S-boxes в каждой дифференциальной характеристике

Линейный анализ: История

- Разработан Митцуру Матцуи (Mitsuru Matsui) в 1992 г.

Митцуру Матцуи

Линейный анализ: Основные идеи

- Known plaintext attack
- Ищем линейную зависимость между исходным текстом, шифротекстом и ключом

$$(x_{\alpha_1} \oplus x_{\alpha_1} \oplus \ldots \oplus x_{\alpha_a}) \oplus (y_{\beta_1} \oplus y_{\beta_2} \oplus \ldots \oplus y_{\beta_b}) = (K_{\gamma_1} \oplus K_{\gamma_1} \oplus \ldots \oplus K_{\gamma_c})$$

- Затем проделываем key-recovery

Линейный анализ: Более подробно

- Анализируем нелинейные компоненты шифра, находим вероятности линейных зависимостей между входными и выходными битами
- Комбинируем полученные зависимости так, чтобы остались только биты исходного текста, шифротекста и ключа
- Вероятность нахождения такой комбинации = $\frac{1}{2} + 2^{n-1} \prod_{i=1}^{n} (p_i - \frac{1}{2})$ (Piling-Up Lemma)
- Key-recovery на DES проходит при использовании 2^{43} известных исходных текстов
- Защита – минимизировать вероятностные смещения (bias), максимизировать число S-boxes, или иных нелинейных элементов

Развитие методов дифференциального и линейного анализа

- Дифференциально-линейный криптоанализ
  - chosen plaintext
  - использует результаты линейного анализа для нахождения дифференциальной характеристики
  - 10 бит ключа 8-раундового DES вскрываются с помощью всего 512 входных текстов
  - защита – быстрое перемешивание (на первых 2-3 раундах)
- Усеченные (truncated) дифференциалы
  - следим лишь за частью битов
- Дифференциалы высших порядков
  - обобщение понятия дифференциальной характеристики
  - например, против f(x)=(x+k)^2 mod p
  - защита – много раундов, функции более высоких порядков
- Невозможные дифф-лы (Miss-in-the-middle attack)
  - ищем дифференциалы, которые заведомо не встретятся, получаем целые классы неподходящих ключей
- Метод бумеранга
  - ищем 2 дифф.характеристики с хорошими вероятностями, покрывающие весь шифр (необходима атака типа chosen-ciphertext)

Интерполяционная атака

- Авторы – Т.Джекобсен и Л.Кнудсен, 1997 год
- Known-text attack
- Предполагаем, что раундовая функция – многочлен. Тогда весь шифр может быть записан как многочлен, коэфф-ты зависят от ключа.
- Интерполируем этот многочлен по достаточно большому количеству исходных текстов

$$f(x) = \sum_{i=1}^{n} y_i \prod_{1 \le j \le n, j \ne i} \frac{x - x_j}{x_i - x_j}$$

Методы, основанные на слабости ключевых разверток

- Метод согласования (Meet-in-the-middle)
  - биты ключа, используемые на 1м и последнем раундах не пересекаются)
- Слабые (weak) и полу-слабые (semi-weak) ключи
  - ключи, для которых результат шифрования сообщения совпадает с результатом расшифрования
  - таких ключей немного, их просто нужно избегать
- Метод связанных ключей
  - Chosen-plaintext attack
  - у нас есть возможность шифровать несколькими ключами, связанными между собой

Будущее криптоанализа

- Алгоритм AES (Rijndael) – современный американский стандарт шифрования
- Он фактически защищен от всех представленных выше атак
- Однако, и на него уже делаются попытки атак, использующие сложные алгебраические теории: Square-saturation-integral-multiset attacks
- Например Square attack, созданный против алгоритма Square – атакует . Chosen plaintext attack, основанный на хорошем выборе множества исходных текстов
  - основной используемый объект - мультимножество
  - особенность: информация получается лишь при рассмотрении всего множества исходных текстов

Vincent Rijmen

J. Daemen

Источники дополнительных сведений

Что и где почитать:

- Bruce Schneier “Self-Study Course in Block Cipher Cryptanalysis”, 2000
  http://www.counterpane.com/self-study.html
  - курс молодого бойца, т.е. для тех, кто хочет реально заняться криптоанализом
- http://www.distributed.net
  - знаменитые взломщики RC5 – просто посмотреть и насладиться =)
- Francois-Xavier Standaert & others “Cryptanalysis of Block Ciphers: the Survey”, 2001
  http://logic.pdmi.ras.ru/~yura/crypto/01crypto.pdf
  - самый полный обзор методов криптоанализа, однако много опечаток и непонятных мест
- Dave Rudolf “Development and Analysis of Block Ciphers and the DES System”, 2002
  http://www.cs.usask.ca/grads/dtr467/400
  - очень понятное введение в основы блочных шифров, внятно описан DES
- М. Анохин, «Блочные криптографические алгоритмы»
  http://www.cryptography.ru/db/msg.html?mid=1162999&uri=node4.html
  - отличный краткий обзор истории и современного состояния криптоанализа, ко всему прочему (УРА!) на русском языке