Новосибирский Государственный Университет
Факультет Информационных Технологий

Разработка white-box криптографической системы

Научный руководитель:
канд. физ.-мат. наук, доцент НГУ
Кренделев С. Ф.

Выполнил:
Арыков Н.Е., НГУ ФИТ, 4 курс

Предметная область

Статистика по массовым утечкам баз данных паролей

Сервер / Владелец	Год	Средняя длина пароля	Паролей проверено	Процент нахождения, [%]	Хеш-функция
Yahoo	2012	8	453000	-	Открытый текст
LinkedIn	2012	-	6500000	58	SHA-1
Last.fm	2012	-	17300000	95	MD5
Formspring	2012	-	420000	-	SHA-256

Проблемы:

- Высокая скорость вычисления хеш-функций
- Малое количество используемых параметров
  - Хеш-функция
  - Соль

25 GPU кластер построенный на OpenCL / MOSIX

Скорость перебора	
SHA-1	**63 Гигабайт/сек**
MD5	**180 Гигабайт/сек**
NTLM	**384 Гигабайт/сек**

Цель работы

- Разработать криптографический протокол, зависящий от большого количества входных параметров, устойчивый к массовому перебору зашифрованных данных
- Реализовать приложения для шифрования данных:
  - White-box шифратор
  - Плагин для СУБД MySQL и веб-интерфейса phpMyAdmin

Существующие решения

Хеш-функции

- Небольшое количество хеш-функций(MD5, SHA-1, SHA-2, RIPEMD-256, Bcrypt)
- Коллизии первого и второго рода
- Два параметра: тип функции и соль
- Соль хранится в открытом виде, обычно, рядом с паролем

Существующие решения

Криптосистемы с открытым ключом

- Три параметра: тип функции, модуль и секретная экспонента (RSA)
- Отсутствует проблема коллизий
- Малое количество криптосистем
- Гомоморфность умножения(RSA, ElGamal)
  - $(m_1 * m_2)^e = m_1^e * m_2^e = c_1 * c_2 (\mathrm{mod}\ n)$, где m1, m2 – открытые тексты; c1, c2 – зашифрованные тексты
- Атака на циклы (RSA)

Биективные отображения

- cx, $x+1$, x^{p-2} для Z_p, где p - простое
- x^n <=> НОД(n, q-1) = 1 для поля Z_q

- Комбинация отображений $P(x) = (ax+b)^e+d$, где $a \in Z_p$, $a \neq 0$, b,d – произвольные элементы из Z_p, e – обратимый элемент из Z_{p-1}

Биективные отображения

- Перестановочный многочлен над полем:
  - Для поля Z_{17} – перестановочных многочленов 17!
  - Максимальная степень многочлена равна 16
  - Базовые многочлены вида x^n являются взаимно однозначными при n=1,3,5,7,9,11,13,15

Схема шифрования

- Фиксируются простые числа $p_1,..,p_r$. Их произведение – модуль n
- Для каждого простого числа p_i выбираются элементарные полиномы над Z_{pi} и вычисляется $F_{p_i}(x) \equiv f_1^{p_i}(...(f_d^{p_i}(x)...)(\mathrm{mod}\, Z_{p_i})$
- После раскрытия скобок в $F_{pi}(x)$ получается биективный полином
- Используя китайскую теорему об остатках вычисляется полином F(x) над Z_n:

  $F(x) = F_{pi}(\mathrm{mod}\ pi)$, i=1…n

Схема шифрования

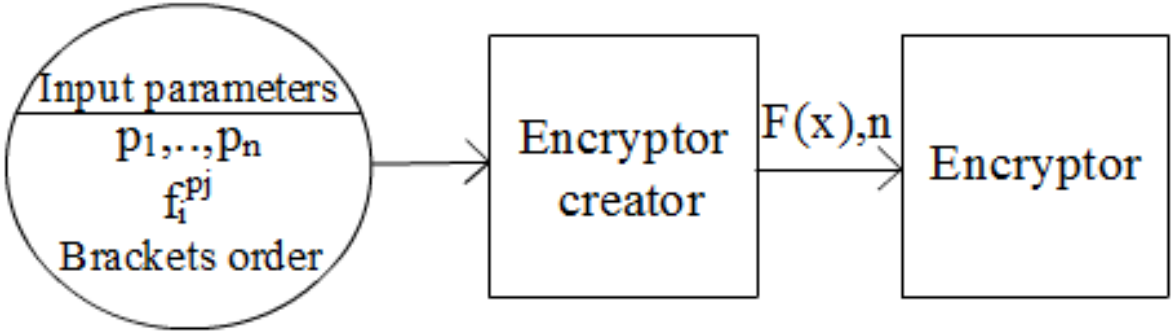
- Публичный ключ – (F, n)
- Приватный ключ состоит из простых чисел, элементарных полиномов и порядка раскрытия скобок.
- Пусть Боб обладает публичным ключом Алисы (F, n) и хочет передать ей сообщение m. Боб вычисляет шифротекст $c=F(m)(\mathrm{mod}\ n)$ и передает его Алисе.

Безопасность криптосистемы

- Отсутствует гомоморфность => система устойчива к атакам по выбранному шифротексту и адаптивно подобранному шифротексту
- Задача факторизации и разложения многочлена на множители
- Большое количество секретных параметров
- Устойчивость к атаке на циклы
- Невозможность прямого перебора, т.к. вид функции неизвестен

Реализация модуля шифрования

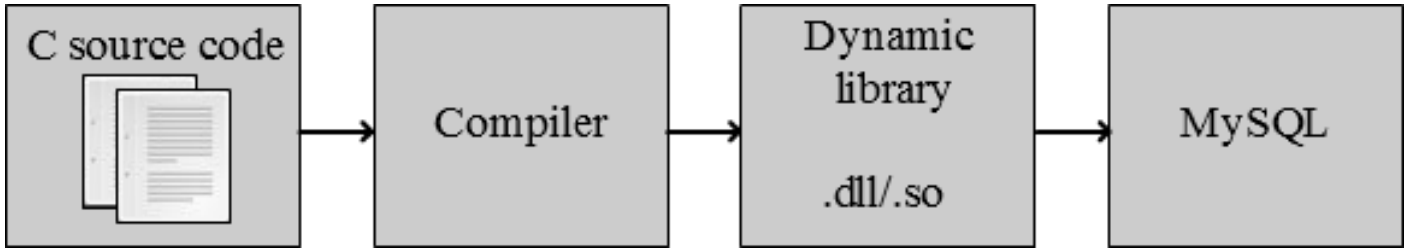
- Программа "Encryptor creator" для создания новой программы "Encryptor”
- "Encryptor" содержит биективный многочлен и модуль.



- Средства: Python, PyQt, UnitTests

Реализация

- Плагин для СУБД MySQL и веб-интерфейса phpMyAdmin. Шифрование реализовано в виде триггера, позволяющего шифровать кортежи и отношения в базе данных.



- Средства: C99, PHP, MySQL/UDF

Дальнейшее развитие системы

- В дальнейшем криптосистему планируется сделать вероятностной, что позволит принципиально усилить шифрование.

$C_1 = E_К(m)$, $C_2 = E_К(m)$, ..., $C_N = E_К(m)$

$m = D_K(C_1) = D_K(C_2) = ... = D_K(C_N)$

Публикации

- 3 место в конкурсе студенческих докладов на РусКрипто’2013, работа представлена к публикации в журнале “Системы высокой доступности”, издаваемом под редакцией ВАК
- Диплом первой степени на МНСК 2013
- Работа была представлена в финале секции Young School международного форума по практической безопасности PHD’2013 и представлена к публикации в журнале “Безопасность информационных технологий”, издаваемом под редакцией ВАК

Новосибирский Государственный Университет
Факультет Информационных Технологий

Разработка white-box криптографической системы

Научный руководитель:
канд. физ.-мат. наук, доцент НГУ
Кренделев С. Ф.

Выполнил:
Арыков Н.Е., НГУ ФИТ, 4 курс