Ежегодная международная научно-практическая конференция
«РусКрипто’2019»

Внедрение закладок в генератор ключей RSA

Маркелова Александра,
к.ф.-м.н.

НТЦ Альфа-Проект

Асимметричная закладка (SETUP-механизм)

Жуков А.Е. Криптосистемы со встроенными лазейками. BYTE Россия, февраль 2007 (№101), с.45-51.

C – исходная криптосистема. C1 – SETUP-механизм:

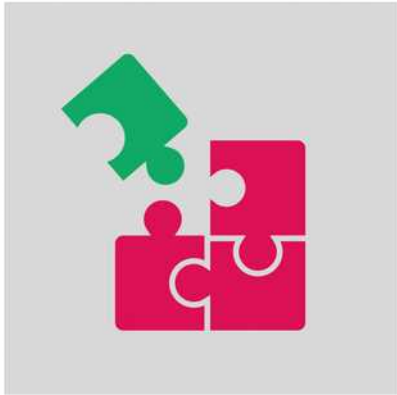
- Параметры входа и выхода C1 согласуются с параметрами C
- Выход C1 содержит дополнительно некоторые зашифрованные секретные биты Bs
- Выход C1 эффективно вычисляется с использованием встроенной в C1 функции шифрования E с открытым ключом
- Секретная функция расшифрования D, обратная к E и необходимая для вычисления Bs, не содержится в C1 и известна только разработчику

SETUP: PAP (Pretty-Awful-Privacy)

Young A., Yung M. Malicious Cryptography. Exposing Cryptovirology. Wiley Publishing, Inc. 2004

- Передаёт информацию о ключе через старшие биты открытого модуля
- Обладает хорошими статистическими свойствами
- Ключ закладки — это RSA ключ длины вдвое меньше, чем ключи в инфицируемой системе
- Предположительно — сниженная скорость работы

Закладка Андерсона



Anderson R. A practical RSA trapdoor. Electronics Letters, 29(11):995, 1993

Kaliski B. S. Anderson's RSA trapdoor can be broken. Electronics Letters, 29(15):1387, 1993

RSA-512 (256-битные простые числа)

D — ключ закладки, 200 бит

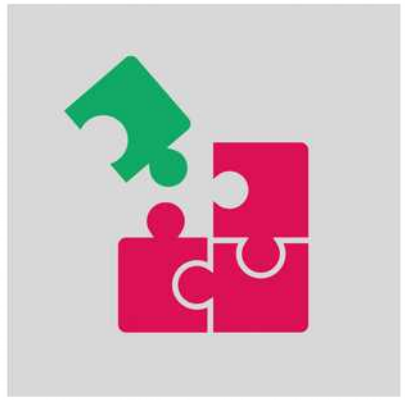
$r(a, D): Z_D^* \times Z_2^{200} \rightarrow Z_2^{56}$

$a_p, a_q < \sqrt{D}, (a_p, D)=(a_q, D)=1$

$$p = r(a_p, D) \cdot D + a_p$$

$$q = r(a_q, D) \cdot D + a_q$$

Закладка Андерсона: вычисление ключей



$$p = r(a_p, D) \cdot D + a_p$$

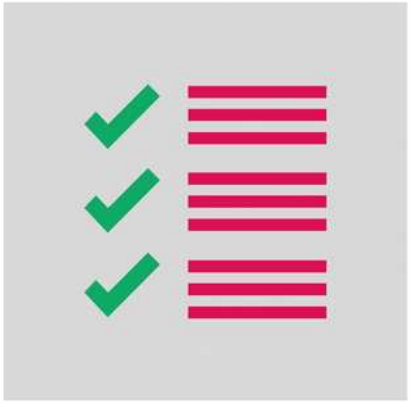
$$q = r(a_q, D) \cdot D + a_q$$

$$n = pq = r(a_p, D) r(a_q, D) D^2 + a_p r(a_q, D) D + a_q r(a_p, D) D + a_p a_q$$

$$n \equiv a_p a_q \bmod D$$

$a_p, a_q < \sqrt{D} \rightarrow a_p a_q < D \rightarrow n \bmod D = a_p a_q$ — 200-битное число

Обозначения



- L — битовая длина открытого RSA-модуля, $|p| = |q| = L/2$
- D — параметр закладки (не обязательно секретный), $|D| = K$
- ID — идентификатор генератора, $|ID|=m$
- i — счётчик генераций
- s — закрытый ключ закладки
- S — открытый ключ закладки (встроен в реализацию)
- $\psi_s(\cdot): Z_D^* \times Z_2^m \times N \to Z_D^*$ — однонаправленная функция (по первому аргументу) с секретом s
- $R(x, y, z, i): Z_2^K \times Z_2^K \times Z_2^m \times N \to Z_2^{L/2-K}$
- $r`(a, D, r_0) = \min \{r \mid r \geq r_0; (rD + a) \text{ — простое}\}$
- $r_{ID}^{(i)}(a, D) = r`(a, D, R(a, D, ID, i))$

Асимметричная закладка, D — любое

1. Выбрать случайно a_p: $a_p < D, (a_p, D)=1$
2. Вычислить: $r_p = r_{ID}^{(i)} (a_p, D)$

   $p = r_p D + a_p$
3. Вычислить: $c = \psi_s (a_p, ID, i)$

   $a_q = c a_p^{-1} \mod D$
4. r_0 — случайно, вычислить: $r_q = r` (a_q, D, r_0)$

   $q = r_q D + a_q$

Вычисление закрытых ключей

$$n = pq = r_p r_q D^2 + a_p r_q D + a_q r_p D + a_p a_q$$

$$n \equiv a_p a_q \equiv c \bmod D$$

$$n \bmod D = c$$

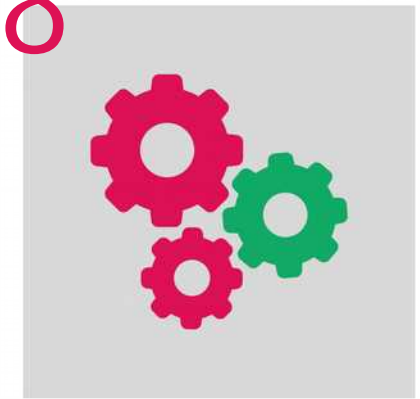
$$a_p = \psi_s^{-1}(c, ID, i)$$

$$r_p = r_{ID}^{(i)}(a_p, D)$$

$$p = r_p D + a_p$$

$$q = n/p$$

Асимметричная закладка, $D=\prod p_i^{\alpha_i}$, $p_i<\delta$



1. Выбрать случайно a_p: $a_p<\lambda(D)$
2. Вычислить: $a(p)=g^{a_p} \bmod D$

   $r_p = r_{ID}^{(i)}(a(p), D), \qquad p = r_p D + a(p)$
3. Вычислить: $c = \psi_s(a_p, ID, i)$

   $a_q = c - a_p \bmod \lambda(D)$
4. r_0 — случайно, вычислить: $a(q) = g^{a_q} \bmod D$

   $r_q = r`(a(q), D, r_0), \qquad q = r_q D + a(q)$

Вычисление закрытых ключей

$$n = pq = r_p r_q D^2 + a(p) r_q D + a(q) r_p D + a(p)a(q)$$

$$n \equiv a(p)a(q) \equiv g^{a_p + a_q} \equiv g^c \bmod D$$

$$c = \mathrm{dlog}_g(n)$$

$$a_p = \psi_s^{-1}(c, ID, i)$$

$$r_p = r_{ID}^{(i)}(g^{a_p} \bmod D, D)$$

$$p = r_p D + (g^{a_p} \bmod D)$$

$$q = n/p$$

ROCA: RSALib, Infineon

Nemec M., Sys M., Svenda P., Klinec D., Matyas V. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. CCS'17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, p. 1631-1648.

- Ключи в RSALib имеют вид:

  $p = k \cdot M + (65537^{\,a} \bmod M)$

  $q = l \cdot M + (65537^{\,b} \bmod M)$

  $n = s \cdot M + (65537^{\,a+b} \bmod M)$

- $M = P_m = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_m$

Key size	M
512 b	$P_{39}\# = 167\#$
1024 b	$P_{71}\# = 353\#$
2048 b	$P_{126}\# = 701\#$
3072 b	$P_{126}\# = 701\#$
4096 b	$P_{225}\# = 1427\#$

Выбор функции ψ_s

- ψ_s — RSA-шифрование

- ψ_s — на основе дискретного логарифмирования:

  $G=\langle g_0 \rangle$ – конечная циклическая группа

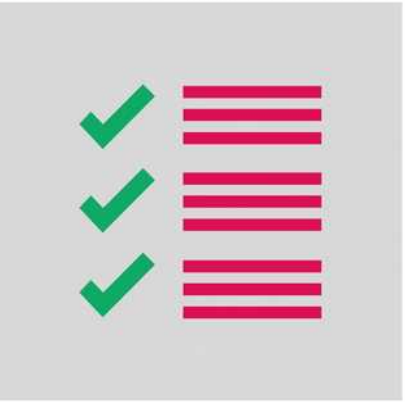
  $\gamma: G \to Z_{\lambda(D)}$ $\quad \theta_\gamma(a)=\{g_i \mid \gamma(g_i)=a\}$

  $S=g_0^{\ s}$ для некоторого секрета s

  $\psi_s(a)=\gamma(g_0^{\ c0})$, где $a = \gamma(S^{c0})$

  $\psi_s^{-1}(c)=\gamma(g_i^{\ s})$, где $g_i \in \theta_\gamma(c)$

Оценка времени работы: аппаратная платформа



P5CD016/021/041 and P5Cx081 family. Secure dual interface and contact PKI smart card controller. Product short data sheet. Rev. 01 — 2 March 2010. PUBLIC

- тактовая частота криптографического сопроцессора FameXE — до 72 мГц
- оперативной памяти (RAM) — 7,5 кБайт, включая 2,5 кБайта памяти криптографического сопроцессора (FXRAM)

Оценка времени работы (RSA-1024)

		Генератор без закладки	Закладка Андерсона	ROCA	Асимметричная закладка
Количество кандидатов	Среднее значение	87	84	34	33
	Минимальное значение	1	1	1	1
	Максимальное значение	596	581	199	209
Время работы	Среднее значение	6,78	6,83	3,23	3,24
	Минимальное значение	1,05	1,23	1,09	1,06
	Максимальное значение	25,81	23,48	11,45	13,24

Вопросы