Низ крипто-системи

Владимир Божовић

Одсјек за математику
Природно-математички факултет

КРИПТОГРАФИЈА

Низ крипто-системи

Као што само име сугерише, низ (stream) крипто-системи врше енкрипцију бит по бит. Због једноставне имплементације и ефикасности, низ крипто-системи су постали стандард у енкрипцији гласа у GSM мрежама.

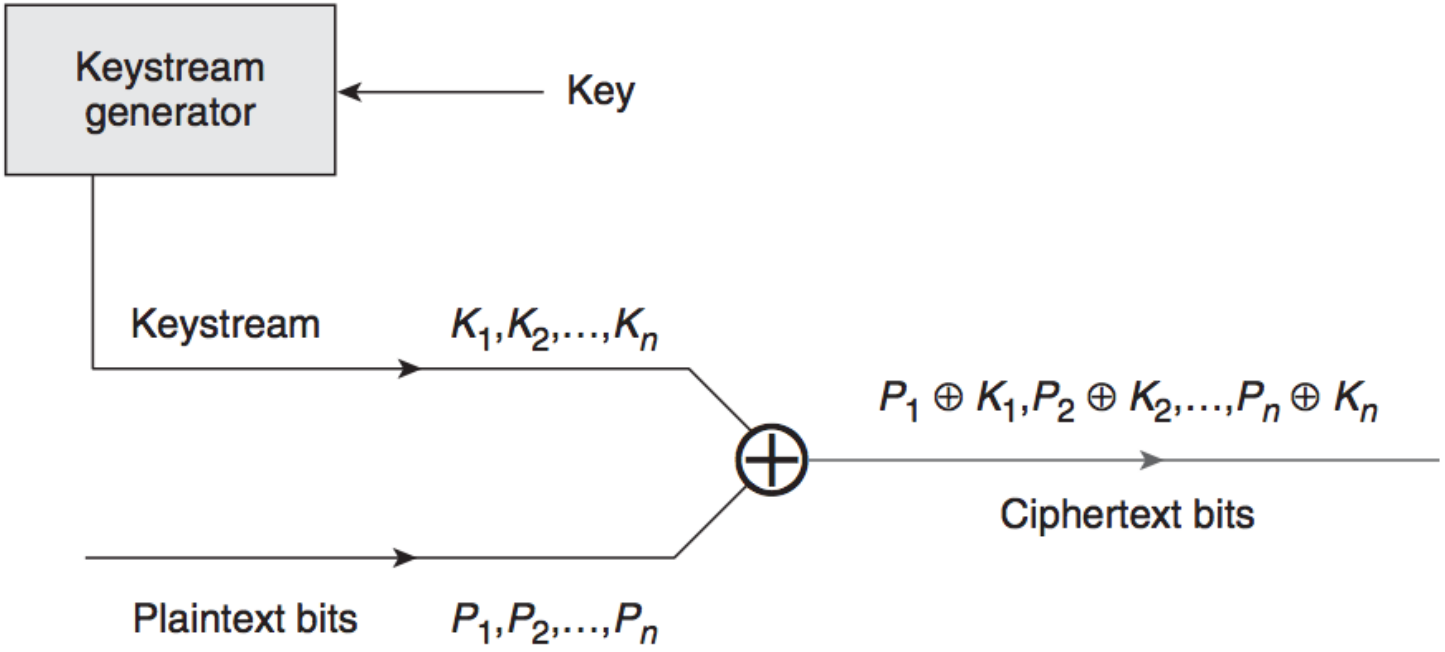
Дефиниција низ крипто-система

На сваки бит x_i поруке $m = (x_1, x_2, \ldots, x_\ell)$ се сабере по модулу 2 одговарајући бит k_i из низа који представља тајни кључ $k = (k_1, k_2, \ldots, k_\ell)$.

Енкрипција:
$E_k(m) = c = (c_1, c_2, \ldots, c_\ell) = (x_1 \oplus k_1, x_2 \oplus k_2, \ldots, x_\ell \oplus k_\ell)$.

Декрипција:
$D_k(c) = (c_1 \oplus k_1, c_2 \oplus k_2, \ldots, c_\ell \oplus k_\ell) = (x_1, x_2, \ldots, x_\ell) = m$.

Примјер: низ крипто-систем



LFSR крипто-систем

Један од најпознатијих представника класе низ крипто система је свакако Linear Feedback Shift Register (LFSR).

Математички опис LFSR крипто-система

1. LFSR почиње са низом битова $s_0, s_1, \ldots, s_{m-1}$.
2. Низ битова је генерисан помоћу формуле

$$s_{i+m} = \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \pmod 2, \quad i = 0, 1, \ldots$$

гдје су $p_j \in \{0, 1\}, \ \ j = 0, 1, \ldots, m-1$ константе које чине суштину конкретне имплементације LFSR-а.

Недостаци LFSR-а

Особине LFSR алгоритма:

- Аргумент линеарне рекурентне формуле у LFSR-у се састоји од m битова.
- Неминовност понављања секвенци у LFSR излазу.
- Максимални период у линеарној рекурзији дубине m је $2^m - 1$.

Примјер максималног периода

Нека је LFSR дефинисан помоћу коефицијената $p_0 = 1, p_1 = 1, p_2 = 0, p_3 = 0$. Његов период је максималан, тј. једнак 15.

Напад на LFSR

Основни правци напада на LFSR користе његову линеарност. Циљ нападача, Оскара, је да дође до $p_0, p_1, \ldots, p_{m-1}$ што заправо представља кључ LFSR-а.

- Претпостављамо да Оскар има приступ LFSR модулу за енкрипцију.
- Оскар може да произведе произвољно много енкрипција и претпостављамо да зна m.
- Чак и ако не зна m, представићемо врло успјешан напад, тако да Оскар може пробати различите вриједности док не дође до рјешења.

Напад на LFSR

Оскар полази од (x_i, y_i) парова бит енкрипција, $E(x_i) = y_i$, за $i = 0, 1, \ldots, 2m-1$. Помоћу овог Оскар реконструише првих $2m$ битова

$$s_i \equiv x_i + y_i \pmod 2, \quad i = 0, 1, \ldots, 2m-1.$$

Као што смо нагласили, циљ нападача је да дође до $p_0, p_1, \ldots, p_{m-1}$, у чијем откривању Оскар користи рекурентну везу

$$s_{i+m} = \sum_{j=0}^{m-1} p_j \cdot s_{i+j} \pmod 2, \quad i = 0, 1, \ldots$$

Напад на LFSR

На основу знања $s_i,\ i = 0, 1, \ldots, 2m-1$ могуће је формирати једначине

$$
\begin{array}{llll}
i = 0, & s_m & \equiv & p_{m-1}s_{m-1} + \cdots p_1 s_1 + p_0 s_0 \pmod 2 \\
i = 1, & s_{m+1} & \equiv & p_{m-1}s_m + \cdots p_1 s_2 + p_0 s_1 \pmod 2 \\
. & . & . & . \quad . \\
. & . & . & . \quad . \\
. & . & . & . \quad . \\
i = m-1, & s_{2m-1} & \equiv & p_{m-1}s_{2m-2} + \cdots p_1 s_m + p_0 s_{m-1} \pmod 2
\end{array}
$$

Сад Оскар има m линеарних једначина са m непознатих $p_0, p_1, \ldots, p_{m-1}$ који је могуће ријешити помоћу Гаусове елиминације, матричним или било којим другим методом.

Нови низ крипто-системи

- Рон Ривест је 1987. предложио другачији дизајн и приступ у односу на LFSR. Убрзо, тај предлог је постао стандард у многим врло затсупњеним апликацијама као што су Microsoft Windows или Oracle SQL.
- Овај низ крипто-систем се дуго користио у Wired Equivalent Privacy (WEP) протоколу, који се користи у wireless мрежама, као и у SSL и TLS протоколима који се користе на вебу.
- Тај крипто-систем је назван RC4 и дуго је био један од најзаступљенијих у пракси, до појаве неких напада који га све више избацају из употребе.
- Дизајнерски критеријуми RC4 се чувају као тајна компаније RSA Security, Inc.

RC4 или ARCFOUR?

- Source код за RC4 се појавио анонимно на Cypherpunks мејлинг листи.
- Коректност овог неофицијелног кода је касније потврђена поређењем резултата са лиценцираном имплементацијом.
- Због заштите ауторских права и могућих правних импликација, овај анонимни код се именује као ARCFOUR.
- ARCFOUR је низ крипто-систем помоћу којег се генерише псеудо-случајни низ који се додаје на основну поруку по модулу 2.

Опис ARCFOUR крипто-система

За генерисање псеудо-случајног низа, ARCFOUR користи низ S од 256 бајтова иницијализован на једноставан начин, помоћу

$$S[i] = i, \quad i = 0, 1, \ldots, 255,$$

као и низ k, такође дужине 256 бајтова који се попуњава одабраним кључем, при чему се бајтови могу понављати. Затим се S трансформише помоћу следећег алгоритма.

Улаз: S

---

j=0

for i=0 to 255 do

$j \leftarrow (j + S[i] + k[i \text{ mod дужина кључа}]) \pmod{256}$

$S[i] \leftrightarrow S[j]$

Излаз: S

Опис ARCFOUR крипто-система

Следећи алгоритам избаца бајт k којим се енкриптује следећи бајт у низу основне поруке. Поступак се може понављати произвољан број пута.

Улаз: S

$i = 0, j = 0$

while GeneratingOutput

$\quad i \leftarrow (i + 1) \pmod{256}$

$\quad j \leftarrow (j + S[i]) \pmod{256}$

$\quad S[i] \leftrightarrow S[j]$

$\quad t \leftarrow (S[i] + S[j]) \pmod{256}$

$\quad k \leftarrow S[t]$

$\quad$ **output** k

end while

Случајно генерисани низ и One-time pad

Један од кључних проблема у криптографији је како генерисати **добар низ**, случајан низ битова, у смислу статистичког критеријума случајности. One-time pad је крипто-систем који суштински зависи од постојања генератора случајног низа битова.

One-time pad

За дату поруку $m = m_1 m_2 \dots m_k$ и случајно генерисани низ $s = s_1 s_2 \dots s_k$, енкрипција се дефинише са

$$c = c_1 c_2 \dots c_k, \quad \text{гдје је } c_i = m_i \oplus s_i, \quad i = 1, 2, \dots, k.$$

One-time pad

У криптографији генерално, постоји одређен ниво реципроцитета између сигурности и ефикасности. One-time pad је, у том смислу, врло упечатљив примјер.

- Доказана апсолутна сигурност one-time pad-а уколико се обезбиједи статистички потпуно случајан низ (Шанонова теорија).
- Различити методи генерисања псеудо-случајних низова.
- Проблем са ефикасношћу one-time pad-а.
- eSTREAM Пројекат (2004. започет, 2008. завршен конкурс). Одабрана четири софтверска и три хардверска рјешења.

Основна подјела генератора случајних низова

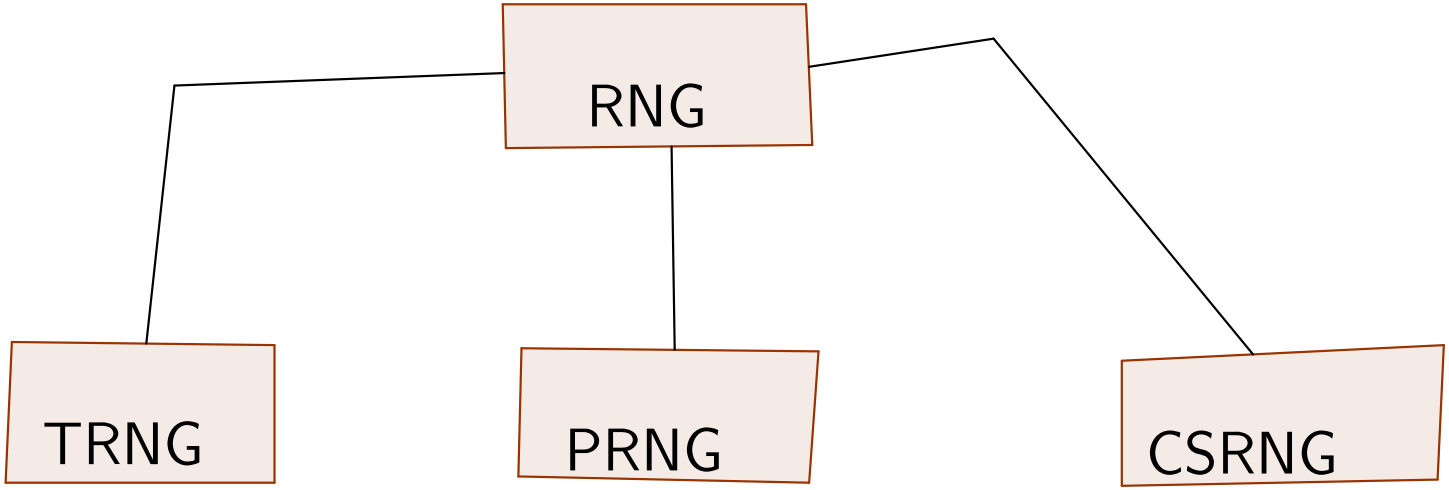


Figure: Подјела генератора случајних низова

Подјела генератора случајних низова

- TRNG (true random number generator)
  Ово је симулирано бацањем новчића.
- PRNG (pseudo random number generators)
  Алгоритам за генерисање "случјних" (ANSI C)
  $s_0 = 12345$
  $s_{i+1} = 1103515245 s_i + 12345 \pmod{2^{33}}, \ i = 0, 1, \ldots$
- CSPRNG (cryptograph. secure PRNG)
  Ако је дато n узастопних битова, онда не постоји алгоритам који се извшава у полиномном времену и предвиђа следећи бит са вјероватноћом изнад 50 посто.
- chi-square тест за мјеру "случајности низа"

Хвала на пажњи :)