Univerzitet u Beogradu
Matematički fakultet

MSEA: Modifikovani simetrični algoritam enkripcije

Seminarski rad

ime i prezime	**Nikola Stanojević**
broj indeksa	1064/2012
predmet	Kriptografija
školska godina	2013/2014
nastavnik	dr Miodrag Živković
datum	10.06.2014

Sadržaj

1 Algoritam

MSEA algoritam je zasnovan na ARX kriptografskom dizajnu. Što znači da su dozvoljene samo elementarne operacije kao što su sabiranje po modulu, rotacije i bitovski XOR (odatle i naziv ARX). MSEA pruža fleksibilnost korisniku omogućavajući mu odabir broja rundi i veličine ulaznog bloka. Rotacije zasnovane na podacima se koriste prilikom enkripcije, dekripcije i prilikom generisanja ključa algoritma MSEA. Ovaj koncept preuzet je od RC5 algoritma.

Sledi opis formiranja, enkripcije u dekripcije MSEA ključa:
Ulazni parametri algoritma:

r: Broj rundi prilikom enkripcije
s: Veličina ulaznog bloka
k: Ključ koji se koristi tokom koraka dvofazne zamene
$\mathbf{M}_k$: Master ključ, koristi se za generisanje ključeva rundi
$\mathbf{K}_1 \dots K_r$: Ključevi rundi korišćeni za procese enkripcije i dekripcije

Koristićemo i sledeće simbole:

R: Rotacije zasnovane na podacima
$\oplus$: Bitovska XOR operacija
$<<<$: Bitovska rotacija ulevo
$>>>$: Bitovska rotacija udesno
$+$: Sabiranje po modulu
$\sim$: Komplement

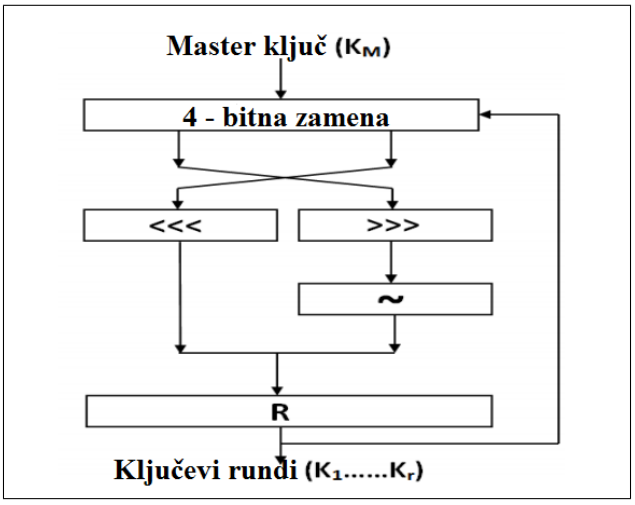
1.1 Formiranje ključa

U algoritmu MSEA koriste se sledeće vrste ključeva:

Ključ zamene (k): Ključ zamene nije uvek iste veličine. Veličina ključa zamene može se izračunati kao: $\log_2 s$, gde s predstavlja veličinu ulaznog bloka. Na primer, za veličinu ulaznog bloka od 128 bita potreban je ključ zamene veličine 7 bita.

Master ključ (M_k): Master ključ se koristi za generisanje ključeva rundi za MSEA proces enkripcije i dekripcije. Veličina master ključa je $2 * s$ bita. Na primer, za veličinu ulaznog bloka od 128 bita potreban je master ključ veličine 256 bita.

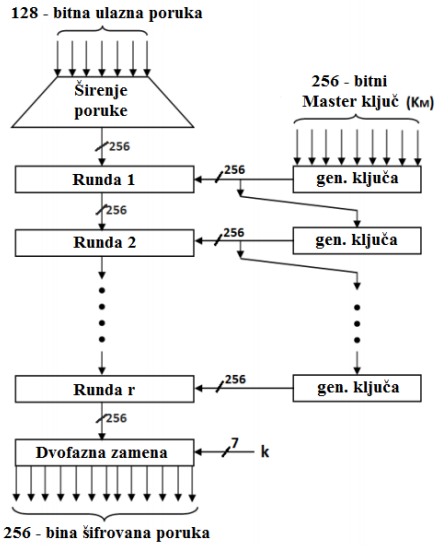
Ključevi rundi ($K_1 \dots K_r$): U MSEA algoritmu broj ključeva rundi zavisi direktno od ulaznog parametra r, gde r predstavlja broj rundi prilikom procesa enkripcije ili dekripcije. Dakle, za svaku rundu postoji jedinstveni ključ te runde. Veličina svakog ključa runde je jednaka veličini master ključa.



Slika 1: Proces generisanja ključeva rundi

1.2 MSEA Enkripcija

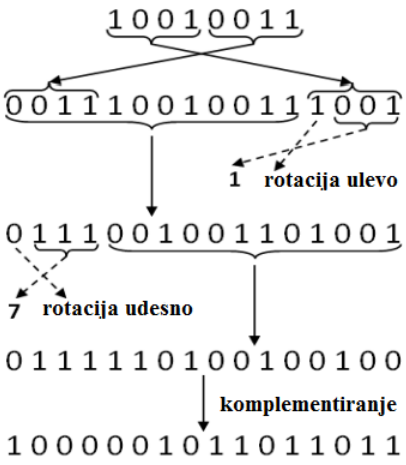
MSEA enkripcija se odvija u tri koraka. Prvi korak je širenje poruke, u drugom koraku se odvijaju funkcije rundi enkripcije a poslednji treći korak je korak dvofazne zamene. Funkcija rundi predstavlja jezgro MSEA enkripcije.



Slika 2: Dijagram enkripcije 128 - bitne poruke

1.2.1 Širenje poruke

U ovoj fazi blok ulazne poruke se proširuje. Svaki 8 - bitni podblok ulazne poruke se proširuje na 16 - bitni podblok, nad kojim je prtitom izvršena rotacija i komplentiranje.



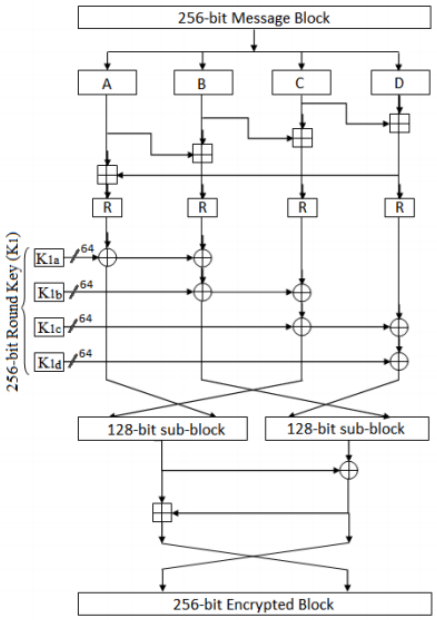
Slika 3: Faza širenja ulazne poruke

1.2.2 Funkcija runde

Sledi pseudokod za funkciju runde pojedinačne runde:

1. podeliti blok ulazne poruke na četiri jednaka dela A,B,C i D
2. D := C + D
3. C := B + C
4. B := A + B
5. A := D + A
6. rotirati A,B,C,D
7. podeliti ključ runde na četiri jednaka dela K_{1a},K_{1b},K_{1c},K_{1d}
8. A := A $\oplus$ K_{1a}
9. B := B $\oplus$ A $\oplus$ K_{1b}
10. C := C $\oplus$ B $\oplus$ K_{1c}
11. D := D $\oplus$ C $\oplus$ K_{1d}

12. konkatenacijom C i A dobijamo E
13. konkatenacijom D i B dobijamo F
14. F := E $\oplus$ F
15. E := E + F
16. konkatenacija F i E



Slika 4: Pojedinačna runda MSEA algoritma

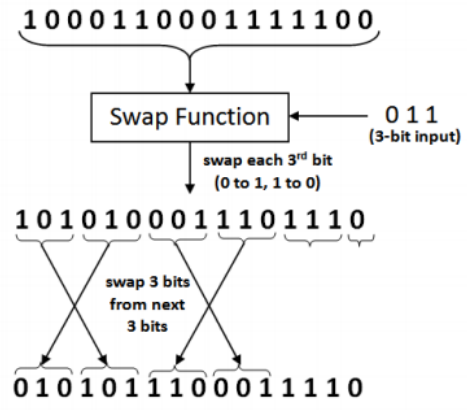
1.2.3 Korak dvofazne zamene

U ovom koraku, koriste se dva tipa operacija koje se obavljaju na osnovu ključa zamene **k**, koji se unosi od strane korisnika:

operacija 1: zameniti svaki k-ti bit bloka poruke u njemu suprotnu binarnu vrednost (0 zameniti u 1, a 1 zameniti u 0).

operacija 2: zameniti svakih k bitova bloka poruke sa narednih k bitova.

Na slici 5 imamo 16-bitni blok poruke **1000110001111100** koji predstavlja ulaz za funkciju zamene sa ključom zamene **011**, što je broj 3 dekadno. U prvoj fazi funkcije zamene svaki treći bit sa ulaza zamenjen je svojom suprotnom binarnom vrednošću. U drugoj fazi funkcije zamene svaki 3-bitni podblok zamenjuje se sa narednim 3-bitnim podblokom.



Slika 5: Funkcija zamene MSEA algoritma

1.3 MSEA Dekripcija

Dekripcija MSEA algoritma je vrlo jednostavna. Izvodi se korišćenjem koraka enkripcije samo u suprotnom smeru. Dakle, prvi korak dekripcije je obrnuti korak dvofazne zamene(prvo se izvrsi operacija 2 pa operacija 1), zatim slede funkcije rundi koristeci obrnutu funkciju runde (kljucevi runde se unose u obrnutom redosledu), na kraju primenjuje se korak skupljanja poruke(suprotan koraku širenja poruke).

2 Reference

1. Cryptology ePrint Archive http://eprint.iacr.org/2014/280.pdf
2. ARX dizajn https://en.wikipedia.org/wiki/Rotational_cryptanalysis