**Visoka strukovna škola za informacione i komunikacione tehnologije**

**Bezbednost informacionih sistema**

****

**Advanced Encryption Standard - RIJNDAEL**

Predmetni profesor: Natalija Vugdelija

Student: Aleksandar Zupčić 279 / 19

Beograd 2019

**SADRŽAJ**

[**1. Kriptografija & DES** 3](#_Toc23672659)

[1.1 Istorija kriptografije 3](#_Toc23672660)

[1.2 DES 4](#_Toc23672661)

[**2. Napadi modernog doba** 4](#_Toc23672662)

[2.1 Vrste napada 4](#_Toc23672663)

[2.2 Brute Force Super Comps 5](#_Toc23672664)

[**3. Uvod u AES** 5](#_Toc23672666)

[3.1 NIST potraga 5](#_Toc23672667)

[3.2 RIJNDAEL 5](#_Toc23672668)

[**4. RIJNDAEL Step By Step** 5](#_Toc23672669)

[4.1 Koraci RIJNDAEL-a 5](#_Toc23672670)

[4.2 ASCII HEX konverzija 5](#_Toc23672671)

[4.3 Sub Bytes 6](#_Toc23672672)

[4.4 Shift Rows 6](#_Toc23672673)

[4.5 Mix Columns 6](#_Toc23672674)

[4.6 Key Schedule & RCON 6](#_Toc23672675)

[4.7 Add Round Key 6](#_Toc23672676)

[**5. Bezbednost AES-a** 6](#_Toc23672677)

[5.1 56 vs 128 6](#_Toc23672678)

[5.2 256 bit 6](#_Toc23672679)

[5.3 Decrypt World 6](#_Toc23672680)

**1. Kriptografija & DES**

## **1.1 Istorija kriptografije**

[1] *“The art and science of concealing the messages to introduce secrecy in information security is recognized as cryptography.”*

Kriptografija je jednom rečenicom “način šifrovanja poruke u skriven i nepoznat oblik”. Sama reč kriptografija se sastoji od dve grčke reči: kripto (skriven/o) i graphene (pisanje/pismo). Međutim, iako je kriptografija grčkog porekla, same početke korišćenja kriptografskog pisma možemo pronaći u Egipatskoj civilizaciji. Jedan od najpoznatijih i najstarijih vrsta kriptografije su hijeroglifi, korišćeni pre četiri milenijuma, čiju su poruku mogli da protumače samo kraljevski pisari. U Evropskim zemljama se koristila mono-alfabetska supstitucija. Jedan od najranijih primera je takozvana Cezarova šifra u kojoj se polja alfabetskih slova pomeraju za određen broj levo ili desno.

Još dva poznata primera kriptografije su:

* Steganografija: za razliku od obične kriptografije u kojoj neku poruku transformišemo i šifrujemo u nepoznat oblik koji druga osoba može da vidi, u steganografiji druga osoba i ne zna da poruka postoji. Jedan od primera moderne steganografije je npr. nevidljivi vodeni žig.
* Enigma: ova vrstu kriptografije su koristili Nemci početkom 20-og veka, za vreme prvog i drugog svetskog rata. Dešifrovanje ovih poruka je donelo velike pobede u borbi protiv nacista. Alan Turing, poznati engleski naučnik, je predvodio dešifrovanje ovih poruka. Nakon Enigme, šifrovanje poruka se sve više radilo na matematički način.

Druge vrste kriptografije: Scytale (koju su koristili Spartanci u 7 veku pre nove ere), Pigpen (geometrijska prosta šifra supstitucije, koju su koristili Masoni), Vigenere (napredna Cezarova šifra, korišćena 1967 godine u Italiji) itd.

*Zanimljivost: Jedan od najranijih primera korišćenja steganografije je Herodot predstavio u njegovim Istorijama. U knjizi se opisuje kako je Histaeus poslao poruku svom vazalu, Aristagorasu, uz pomoć svog roba tako što mu je obrijao glavu, urezao poruku na koži i poslao Aristagorasu roba kada mu je kosa dovoljno porasla. Aristagoras je nakon toga obrijao kosu robu, otkrivajući šifrovanu poruku.*

## **1.2 DES**

Na kraju, postoje i kriptografije modernog doba, kao što su DES (Data Encryption Standard, vrsta kriptografije korišćena krajem 20-og veka) i AES (Advanced Encryption Standard, moderna vrsta kriptografije) koje se danas uveliko koriste sa ciljem bezbednosti važnih informacija.

# **2. Napadi modernog doba**

## **2.1 Vrste napada**

Diferencijalna i linearna kriptoanaliza (DC & LC): Diferencijalnu kriptoanalizu su izumeli Adi Šamir i Eli Biham 1980-te godine. 1993-će godine, Micuri Macui je izumeo linearnu kriptoanalizu. Za DC je navodno potrebno 2 na 49 kombinacija teksta za testiranje. Za LC je predviđeno da postoji 2 na 43.

Dejvijev Napad (DA): Specifično dizajniran za napad na DES algoritme, za razliku od linearne i diferencijalne koji se ne odnose samo na DES strukturu. Kreirao ga je Donald Dejvi 1980-te godine.

Brute Force Attack: Predstavlja najprostiji, najlakši i, do sada, najpraktičniji pešadijski način dešifrovanja poruke svakog sistema. Koristi sve moguće kombinacije i zavisi od broja bita ključa: ključevi sa malim brojem bita su manje otporni zbog broja mogućih kombinacija. Sa pojavom sve jačih, bržih i moćnijih kompjutera, Brute Force Attack dobija na snazi, bio je glavni razlog prelaska sa DES na AES / Rijndael.

## **2.2 Brute Force Super Comps**

# **3. Uvod u AES**

## **3.1 NIST potraga**

## **3.2 RIJNDAEL**

# **4. RIJNDAEL Step By Step**

## **4.1 Koraci RIJNDAEL-a**

Attacksdfsdfsdddd asdasd

|  |  |  |  |
| --- | --- | --- | --- |
| v | k | k |  |
| i | a | o | i |
| s |  | l | c |
| o | s | a | t |

|  |  |  |  |
| --- | --- | --- | --- |
| p | p | c | o |
| e | e | p | v |
| r | r | o | o |
| a | i | n | o |

|  |  |  |  |
| --- | --- | --- | --- |
| 38 | 7F | 7F | B7 |
| F9 | EF | A8 | F9 |
| 8F | B7 | 50 | FB |
| A8 | 8F | EF | 92 |

|  |  |  |  |
| --- | --- | --- | --- |
| 38 | 7F | 7F | B7 |
| F9 | EF | A8 | F9 |
| 8F | B7 | 50 | FB |
| A8 | 8F | EF | 92 |

dasdadasdsadadasdasd

sdfdsfsdfsdfs

## 

## **4.2 ASCII HEX konverzija**

Kako bi mogli da izvršimo predstojeće korake, tekst koji želimo da šifrujemo se prvo heksadecimalno konvertuje korišćenjem ASCII tabele, slovo po slovo, dok se ne popune i konvertuju sva polja.

ASCII tabela

|  |  |  |  |
| --- | --- | --- | --- |
| 76 | 6B | 6B | 20 |
| 69 | 61 | 6F | 69 |
| 73 | 20 | 6C | 63 |
| 6F | 73 | 61 | 74 |

U našem slučaju „visoka skola ict“ to će izgledati ovako. Karakter / Char „v“ se prvo pretvara u heksadecimalnu vrednost 76. Slovo „i“ se pretvara u vrednost 69, što možemo da vidimo i u reči “ict” sa heksadecimalnim vrednostima 69 (i), 63 (c) i 73 (t). Treba takođe obratiti pažnju na veličinu slova. Ako bismo, npr, koristili reč ICT, to bi imalo sasvim drugu vrednost (49 43 54) pošto se velika slova u ASCII tabeli razlikuju i vode drugačije od malih slova.

## **4.3 Sub Bytes**

Heksadecimalne vrednosti se dalje zamenjuju vrednostima po S-Box (Substitute Box) tabeli. Prvo slovo / broj u heksadecimalnoj vrednosti predstavlja njenu Y osu a drugo predstavlja njenu X osu. Korišćenjem tih koordinata nalazimo vrednost heksadecimalnog broja u S-Box tabeli.

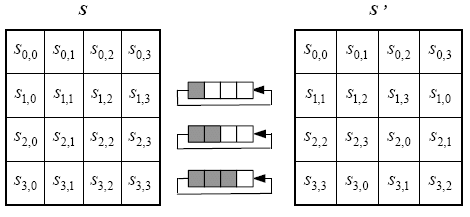
Substitute Box

|  |  |  |  |
| --- | --- | --- | --- |
| 38 | 7F | 7F | B7 |
| F9 | EF | A8 | F9 |
| 8F | B7 | 50 | FB |
| A8 | 8F | EF | 92 |

Polja bita nakon S-Box konverzije.

U našem primeru će to izgledati ovako. Prvo polje prve kolone je pre supstitucije bilo 76, što znači da je njena koordinata 7 (po Y osi) i 6 (po X osi). Koristeći S-Box, nalazimo njenu vrednost u tabeli koja je 38. Isto radimo i za sva ostala polja i prolazimo kroz ukupno 16 koraka.

## **4.4 Shift Rows**

U ovoj fazi, redovi bita se pomeraju ulevo i menjaju mesta po sistemu 0, 1, 2, 3. Prvi red se ne menja. Drugi red se pomera ulevo za jedan, pomerajući prvo polje na kraj. Treći se pomera za dva polja itd.

Shift Rows

|  |  |  |  |
| --- | --- | --- | --- |
| 38 | 7F | 7F | B7 |
| EF | A8 | F9 | F9 |
| 50 | FB | 8F | B7 |
| 92 | A8 | 8F | EF |

asdsad

To će izgledati ovako u našem primeru. U drugom redu, red se vodio kao F9 EF A8 F9 a sada je F9 na poslednjoj poziciji a EF na prvoj. Primetićemo da se prvi red tabele ne menja, i da su vrednosti 7F i 7F blizu jedne drugoj što nije dobro jer može da otkrije neke informacije. Kako bismo ovo sprečili, pošto se prvi red ne menja u ovoj fazi, radimo sledeći korak.

**4.5 Mix Columns**

## **4.6 Key Schedule & RCON**

## **4.7 Add Round Key**

# **5. Bezbednost AES-a**

## **5.1 56 vs 128**

## **5.2 256 bit**

## **5.3 Decrypt World**

*„If you assume:*

* *Every person on the planet owns 10 computers;*
* *There are 7 billion people on the planet;*
* *Each of these computers can test 1 billion key combinations per second;*
* *On average, you can crack the key after testing 50% of the possibilities..*

*..then the earth's population can crack one encryption key in 77,000,000,000,000,000,000,000,000 years!“*

**LITERATURA**

* Формат А4
* маргине: горња, доња, лева и десна по 1“ или 2,5cm
* фонт TimesNewRoman или Arial и следеће величине слова:
  + наслови - велика слова16 pt, bold,
  + поднаслови–14pt,
  + текст – 12 pt,
  + проред 1.5