Криптографија
- четврти део -

доц. др Драган Ђокић

Математички факултет, Универзитет у Београду

dragan.djokic@matf.bg.ac.rs

22. март 2024.

Коначна поља (подсећање)

- $\mathbb{F}_q$ = коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја

Коначна поља (подсећање)

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p

Коначна поља (подсећање)

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- $q = p^d$: $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d

Коначна поља (подсећање)

- $\mathbb{F}_q =$ коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- $q = p^d$: $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d
- $(\mathbb{F}_q^*, \cdot)$ је циклична група, где је $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ састављена од инвертибилних елемената из $\mathbb{F}_q$

Коначна поља (подсећање)

- $\mathbb{F}_q$ = коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- $q = p^d$: $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d
- $(\mathbb{F}_q^*, \cdot)$ је циклична група, где је $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ састављена од инвертибилних елемената из $\mathbb{F}_q$
- За сложен број n: $\mathbb{Z}_n$ је прстен који није поље
  - у $\mathbb{Z}_n$ постоје делитељи нуле који немају инверз
  - Пример: $2 \cdot 3 \equiv 0 \pmod 6$, и 2 и 3 немају инверз по модулу 6

Коначна поља (подсећање)

- $\mathbb{F}_q$ = коначно поље са q елемената (јединствено одређено до на изоморфизам) где је $q = p^d$ степен простог броја
- $\mathbb{F}_p \cong \mathbb{Z}_p$ за прост p
- $q = p^d$: $\mathbb{F}_q \cong \mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$, где је $f(x) \in \mathbb{Z}_p[x]$ нерастављив полином степена d
- $(\mathbb{F}_q^*, \cdot)$ је циклична група, где је $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ састављена од инвертибилних елемената из $\mathbb{F}_q$
- За сложен број n: $\mathbb{Z}_n$ је прстен који није поље
  - у $\mathbb{Z}_n$ постоје делитељи нуле који немају инверз
  - Пример: $2 \cdot 3 \equiv 0 \pmod 6$, и 2 и 3 немају инверз по модулу 6
- Слично, ако f није нерастављив: $\mathbb{Z}_p[x] / (f\mathbb{Z}_p[x])$ је прстен који није поље
  - У $\mathbb{Z}_2[x] / \left(\left(x^2+1\right)\mathbb{Z}_2[x]\right)$ важи $(x+1)^2 = x^2 + 1 = 0$ и $x+1$ нема инверз

Zadatak *odrediti* $(x^4 + x^3 + 1)^{-1}$ *u polju* $\mathbb{F}_2[x]/(x^6 + x + 1)$.

Rešenje: Invertovanje polinoma $q(x)$ nad poljem $\mathbb{F}_2[x]/p(x)$ vrši se primenom Euklidovog algoritma na polinome $p(x)$ i $q(x)$.

$$x^6 + x + 1 = (x^2 + x + 1) \cdot (x^4 + x^3 + 1) + (x^3 + x^2)$$
$$x^4 + x^3 + 1 = x \cdot (x^3 + x^2) + \underline{1}$$

Zatim, određujemo linearnu kombinaciju polinoma koja daje vrednost njihovog NZD-a:

$$\begin{aligned} 1 &= (x^4 + x^3 + 1) + x \cdot (x^3 + x^2) \\ &= (x^4 + x^3 + 1) + x \cdot ((x^6 + x + 1) + (x^2 + x + 1) \cdot (x^4 + x^3 + 1)) \\ &= x \cdot (x^6 + x + 1) + (x^3 + x^2 + x + 1) \cdot (x^4 + x^3 + 1) \end{aligned}$$

Iz linearne kombinacije dobijamo da je $(x^4 + x^3 + 1)^{-1} = (x^3 + x^2 + x + 1)$ u polju $\mathbb{F}_2[x]/(x^6 + x + 1)$.

AES (Advanced Encryption Standard)

- AES је тренутно најраспрострањенији симетричан криптосистем уведен 2001., познат и под именом Rijndael по творцима Рејмену и Дајмену

AES (Advanced Encryption Standard)

- AES је тренутно најраспрострањенији симетричан криптосистем уведен 2001., познат и под именом Rijndael по творцима Рејмену и Дајмену
- Блоковска шифра - криптује блокове од по 128 бита (16 ASCII симбола)
  - приказаћемо поједностављену верзију Simplified AES који криптује блокове од 16 битова
  - За комплетну верзију AES видети Живковић, Глава 12.3

AES (Advanced Encryption Standard)

- AES је тренутно најраспрострањенији симетричан криптосистем уведен 2001., познат и под именом Rijndael по творцима Рејмену и Дајмену
- Блоковска шифра - криптује блокове од по 128 бита (16 ASCII симбола)
  - приказаћемо поједностављену верзију Simplified AES који криптује блокове од 16 битова
  - За комплетну верзију AES видети Живковић, Глава 12.3
- SAES комбинује неколико једноставних криптосистема (OTP, афина, шифра премештањем...) на поруци, али и на кључу

AES (Advanced Encryption Standard)

- AES је тренутно најраспрострањенији симетричан криптосистем уведен 2001., познат и под именом Rijndael по творцима Рејмену и Дајмену
- Блоковска шифра - криптује блокове од по 128 бита (16 ASCII симбола)
  - приказаћемо поједностављену верзију Simplified AES који криптује блокове од 16 битова
  - За комплетну верзију AES видети Живковић, Глава 12.3
- SAES комбинује неколико једноставних криптосистема (OTP, афина, шифра премештањем...) на поруци, али и на кључу
- Нибл $= 4$ бита, бајт $= 8$ битова $= 2$ нибла

Користићемо пресликавање ниблова $S = S_2 \circ S_1$ које је композиција 2 пресликавања:

- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{16} = \mathbb{Z}_2[x] \,/ \left(\left(x^4 + x + 1 \right) \mathbb{Z}_2[x] \right).$ $S_1 \left(b_3b_2b_1b_0 \right)$ ће бити нибл који одговара инверзу од $b_3x^3 + b_2x^2 + b_1x + b_0$ у $\mathbb{F}_{16}$, изузетак је нула-нибл: $S_1(0000) = 0000$

Користићемо пресликавање ниблова $S = S_2 \circ S_1$ које је композиција 2 пресликавања:

- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{16} = \mathbb{Z}_2[x] \,/ \left(\left(x^4 + x + 1 \right) \mathbb{Z}_2[x] \right).$ $S_1 \left(b_3b_2b_1b_0 \right)$ ће бити нибл који одговара инверзу од $b_3x^3 + b_2x^2 + b_1x + b_0$ у $\mathbb{F}_{16}$, изузетак је нула-нибл: $S_1(0000) = 0000$
  - Пример: $S_1(0011) = (x+1)^{-1} = x^3 + x^2 + x = 1110$

Користићемо пресликавање ниблова $S = S_2 \circ S_1$ које је композиција 2 пресликавања:

- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{16} = \mathbb{Z}_2[x] \,/ \left(\left(x^4 + x + 1\right)\mathbb{Z}_2[x]\right)$. $S_1\left(b_3b_2b_1b_0\right)$ ће бити нибл који одговара инверзу од $b_3x^3 + b_2x^2 + b_1x + b_0$ у $\mathbb{F}_{16}$, изузетак је нула-нибл: $S_1(0000) = 0000$
  - Пример: $S_1(0011) = (x+1)^{-1} = x^3 + x^2 + x = 1110$
- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0$ из прстена $\mathbb{Z}_2[x] \,/ \left(\left(x^4 + 1\right)\mathbb{Z}_2[x]\right)$. $S_2\left(b_3b_2b_1b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^3 + x^2 + 1\right)\left(b_3x^3 + b_2x^2 + b_1x + b_0\right) + \left(x^3 + 1\right)$

Користићемо пресликавање ниблова $S = S_2 \circ S_1$ које је композиција 2 пресликавања:

- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{16} = \mathbb{Z}_2[x] \,/ \left(\left(x^4 + x + 1\right)\mathbb{Z}_2[x]\right)$. $S_1\left(b_3b_2b_1b_0\right)$ ће бити нибл који одговара инверзу од $b_3x^3 + b_2x^2 + b_1x + b_0$ у $\mathbb{F}_{16}$, изузетак је нула-нибл: $S_1(0000) = 0000$
  - Пример: $S_1(0011) = (x+1)^{-1} = x^3 + x^2 + x = 1110$
- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0$ из прстена $\mathbb{Z}_2[x] \,/ \left(\left(x^4 + 1\right)\mathbb{Z}_2[x]\right)$. $S_2\left(b_3b_2b_1b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^3 + x^2 + 1\right)\left(b_3x^3 + b_2x^2 + b_1x + b_0\right) + \left(x^3 + 1\right)$
  - Пример: $S_2(1110) = \left(x^3 + x^2 + 1\right)\left(x^3 + x^2 + x\right) + \left(x^3 + 1\right) = x^3 + x + 1 = 1011$

Користићемо пресликавање ниблова $S = S_2 \circ S_1$ које је композиција 2 пресликавања:

- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0 \in \mathbb{F}_{16} = \mathbb{Z}_2[x] / \left(\left(x^4 + x + 1\right)\mathbb{Z}_2[x]\right)$. $S_1\left(b_3b_2b_1b_0\right)$ ће бити нибл који одговара инверзу од $b_3x^3 + b_2x^2 + b_1x + b_0$ у $\mathbb{F}_{16}$, изузетак је нула-нибл: $S_1(0000) = 0000$
  - Пример: $S_1(0011) = (x+1)^{-1} = x^3 + x^2 + x = 1110$
- Нибл $b_3b_2b_1b_0$ се поистовећује са полиномом $b_3x^3 + b_2x^2 + b_1x + b_0$ из прстена $\mathbb{Z}_2[x] / \left(\left(x^4 + 1\right)\mathbb{Z}_2[x]\right)$. $S_2\left(b_3b_2b_1b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^3 + x^2 + 1\right)\left(b_3x^3 + b_2x^2 + b_1x + b_0\right) + \left(x^3 + 1\right)$
  - Пример: $S_2(1110) = \left(x^3 + x^2 + 1\right)\left(x^3 + x^2 + x\right) + \left(x^3 + 1\right) = x^3 + x + 1 = 1011$

S је пример једноставног блоковског криптосистема (овде су кључеви $x^3 + x^2 + 1$ и $x^3 + 1$ фиксирани)

S се може приказати таблично

NIBL	S(NIBL)
0000	1001
0001	0100
0010	1010
0011	1011
0100	1101
0101	0001
0110	1000
0111	0101
1000	0110
1001	0010
1010	0000
1011	0011
1100	1100
1101	1110
1110	1111
1111	0111

S се може приказати таблично

NIBL	S(NIBL)
0000	1001
0001	0100
0010	1010
0011	1011
0100	1101
0101	0001
0110	1000
0111	0101
1000	0110
1001	0010
1010	0000
1011	0011
1100	1100
1101	1110
1110	1111
1111	0111

За комплетан AES би таблица била превелика и непрактична

Проширивање кључа

- SAES користи 16-битни кључ K_0 (који су некако Алиса и Бобан разменили)

Проширивање кључа

- SAES користи 16-битни кључ K_0 (који су некако Алиса и Бобан разменили)
- Помоћу тог кључа се ,,случајно“ генеришу још два кључа K_1 и K_2 исте дужине. Сваки од кључева има по 2 бајта $K_i = W_{2i}W_{2i+1}$, $i = 0, 1, 2$

Проширивање кључа

- SAES користи 16-битни кључ K_0 (који су некако Алиса и Бобан разменили)
- Помоћу тог кључа се ,,случајно“ генеришу још два кључа K_1 и K_2 исте дужине. Сваки од кључева има по 2 бајта $K_i = W_{2i}W_{2i+1},\ i = 0, 1, 2$
- Сваки бајт је састављен од 2 нибла N_0N_1, па ћемо имати пресликавања бајтова $R(N_0N_1) = N_1N_0$ (ротација) и $S(N_0N_1) = S(N_0)\,S(N_1)$, где је S на нибловима већ описано

Проширивање кључа

- SAES користи 16-битни кључ K_0 (који су некако Алиса и Бобан разменили)
- Помоћу тог кључа се ,,случајно“ генеришу још два кључа K_1 и K_2 исте дужине. Сваки од кључева има по 2 бајта $K_i = W_{2i}W_{2i+1},\ i = 0, 1, 2$
- Сваки бајт је састављен од 2 нибла N_0N_1, па ћемо имати пресликавања бајтова $R(N_0N_1) = N_1N_0$ (ротација) и $S(N_0N_1) = S(N_0)\,S(N_1)$, где је S на нибловима већ описано
- Дефинишемо низ бајтова C_i који се добија спајањем нибла који одговара x^{i+2} у $\mathbb{F}_{16} = \mathbb{Z}_2[x] \,/\, \left(\left(x^4 + x + 1\right)\mathbb{Z}_2[x]\right)$ и нибла 0000

Проширивање кључа

- SAES користи 16-битни кључ K_0 (који су некако Алиса и Бобан разменили)
- Помоћу тог кључа се ,,случајно“ генеришу још два кључа K_1 и K_2 исте дужине. Сваки од кључева има по 2 бајта $K_i = W_{2i}W_{2i+1},\ i = 0, 1, 2$
- Сваки бајт је састављен од 2 нибла N_0N_1, па ћемо имати пресликавања бајтова $R(N_0N_1) = N_1N_0$ (ротација) и $S(N_0N_1) = S(N_0)\,S(N_1)$, где је S на нибловима већ описано
- Дефинишемо низ бајтова C_i који се добија спајањем нибла који одговара x^{i+2} у $\mathbb{F}_{16} = \mathbb{Z}_2[x] \,/\, \left(\left(x^4 + x + 1\right)\mathbb{Z}_2[x]\right)$ и нибла 0000
- Бајтови кључа $W_i,\ i = 2, 3, 4, 5$, се добијају као

$$W_i = \begin{cases} W_{i-2} + C_{\frac{i}{2}} + S\left(R\left(W_{i-1}\right)\right), & \text{ако } 2|i \\ W_{i-2} + W_{i-1}, & \text{ако } 2 \nmid i, \end{cases}$$

где је $+$ сабирање нибблова у $\mathbb{F}_{16}$

Пример: $K_0 = \underbrace{0101\ 1001}_{W_0}\ \underbrace{0111\ 1010}_{W_1}$

- $S\left(R\left(W_1\right)\right) = S(1010\ 0111) = 0000\ 0101$
- $W_2 = W_0 + C_1 + S\left(R\left(W_1\right)\right)$
  $= 0101\ 1001 + 1000\ 0000 + 0000\ 0101 = 1101\ 1100$
- $W_3 = W_1 + W_2 = 0111\ 1010 + 1101\ 1100 = 1010\ 0110$
- $K_1 = 1101\ 1100\ 1010\ 0110$

Пример: $K_0 = \underbrace{0101\ 1001}_{W_0}\ \underbrace{0111\ 1010}_{W_1}$

- $S\left(R\left(W_1\right)\right) = S(1010\ 0111) = 0000\ 0101$
- $W_2 = W_0 + C_1 + S\left(R\left(W_1\right)\right)$
  $= 0101\ 1001 + 1000\ 0000 + 0000\ 0101 = 1101\ 1100$
- $W_3 = W_1 + W_2 = 0111\ 1010 + 1101\ 1100 = 1010\ 0110$
- $K_1 = 1101\ 1100\ 1010\ 0110$
- $S\left(R\left(W_3\right)\right) = S(0110\ 1010) = 1000\ 0000$
- $W_4 = W_2 + C_2 + S\left(R\left(W_3\right)\right)$
  $= 1101\ 1100 + 0011\ 0000 + 1000\ 0000 = 0110\ 1100$
- $W_5 = W_3 + W_4 = 1010\ 0110 + 0110\ 1100 = 1100\ 1010$
- $K_2 = 0110\ 1100\ 1100\ 1010$

Примена SAES-а

- Користи сва три 16-битна кључа K_0, K_1, K_2

Примена SAES-а

- Користи сва три 16-битна кључа K_0, K_1, K_2
- Шифрује се отворени текст од 16 бајтова $= 4$ нибла $N_0N_1N_2N_3$ који се обично представља таблично

N_0	N_2
N_1	N_3

Примена SAES-а

- Користи сва три 16-битна кључа K_0, K_1, K_2
- Шифрује се отворени текст од 16 бајтова $= 4$ нибла $N_0N_1N_2N_3$ који се обично представља таблично

N_0	N_2
N_1	N_3

- SAES је композиција 8 функција

$$D_{K_2} \circ Z \circ S \circ D_{K_1} \circ M \circ Z \circ S \circ D_{K_0}$$

  - S као раније, примењује се на сваки нибл N_j појединачно

Примена SAES-а

- Користи сва три 16-битна кључа K_0, K_1, K_2
- Шифрује се отворени текст од 16 бајтова $= 4$ нибла $N_0N_1N_2N_3$ који се обично представља таблично

N_0	N_2
N_1	N_3

- SAES је композиција 8 функција

$$D_{K_2} \circ Z \circ S \circ D_{K_1} \circ M \circ Z \circ S \circ D_{K_0}$$

  - S као раније, примењује се на сваки нибл N_j појединачно
  - D_{K_j}: на $N_0N_1N_2N_3$ се додаје K_j ($+_2$ бит по бит) као OTP

Примена SAES-а

- Користи сва три 16-битна кључа K_0, K_1, K_2
- Шифрује се отворени текст од 16 бајтова $= 4$ нибла $N_0N_1N_2N_3$ који се обично представља таблично

N_0	N_2
N_1	N_3

- SAES је композиција 8 функција

$$D_{K_2} \circ Z \circ S \circ D_{K_1} \circ M \circ Z \circ S \circ D_{K_0}$$

  - S као раније, примењује се на сваки нибл N_j појединачно
  - D_{K_j}: на $N_0N_1N_2N_3$ се додаје K_j ($+_2$ бит по бит) као OTP
  - Z замењује места у другој врсти

$$Z\left(\begin{array}{|c|c|}\hline N_0 & N_2 \\ \hline N_1 & N_3 \\ \hline\end{array}\right) = \begin{array}{|c|c|}\hline N_0 & N_2 \\ \hline N_3 & N_1 \\ \hline\end{array}$$

- M трансформише сваку од колона $\boxed{\begin{array}{c} N_j \\ \hline N_k \end{array}}$ на следећи начин:
  - користи се прстен $\mathbb{F}_{16}[y] \,/\, \left(\left(y^2+1\right)\mathbb{F}_{16}[y]\right)$, или интуитивније записано $\mathbb{F}_{16}[i]$, $i^2 = -1$ $(= 1$ у $\mathbb{F}_{16})$

- M трансформише сваку од колона $\begin{array}{|c|}\hline N_j \\ \hline N_k \\ \hline \end{array}$ на следећи начин:
  - користи се прстен $\mathbb{F}_{16}[y] \,/\, \left(\left(y^2+1\right)\mathbb{F}_{16}[y]\right)$, или интуитивније записано $\mathbb{F}_{16}[i]$, $i^2 = -1$ $(= 1$ у $\mathbb{F}_{16})$
  - колона се поистовећује са $N_j i + N_k$, затим се помножи са $x^2 i + 1$, резултат се запише у облику $Ai + B$, $A, B \in \mathbb{F}_{16}$, и колона $\begin{array}{|c|}\hline A \\ \hline B \\ \hline \end{array}$ је резултат трансформације M

- M трансформише сваку од колона $\boxed{\begin{array}{c} N_j \\ \hline N_k \end{array}}$ на следећи начин:
  - користи се прстен $\mathbb{F}_{16}[y] \,/\, \left(\left(y^2+1\right)\mathbb{F}_{16}[y]\right)$, или интуитивније записано $\mathbb{F}_{16}[i]$, $i^2 = -1$ $(= 1$ у $\mathbb{F}_{16})$
  - колона се поистовећује са $N_j i + N_k$, затим се помножи са $x^2 i + 1$, резултат се запише у облику $Ai + B$, $A, B \in \mathbb{F}_{16}$, и колона $\boxed{\begin{array}{c} A \\ \hline B \end{array}}$ је резултат трансформације M
  - Пример: $M\left(\boxed{\begin{array}{c} 1010 \\ \hline 1001 \end{array}}\right) = \left(\left(x^3+x\right)i + \left(x^3+1\right)\right)\left(x^2 i + 1\right)$

    $= \cdots = x^3 i + \left(x^2 + x + 1\right) = \boxed{\begin{array}{c} 1000 \\ \hline 0111 \end{array}}$

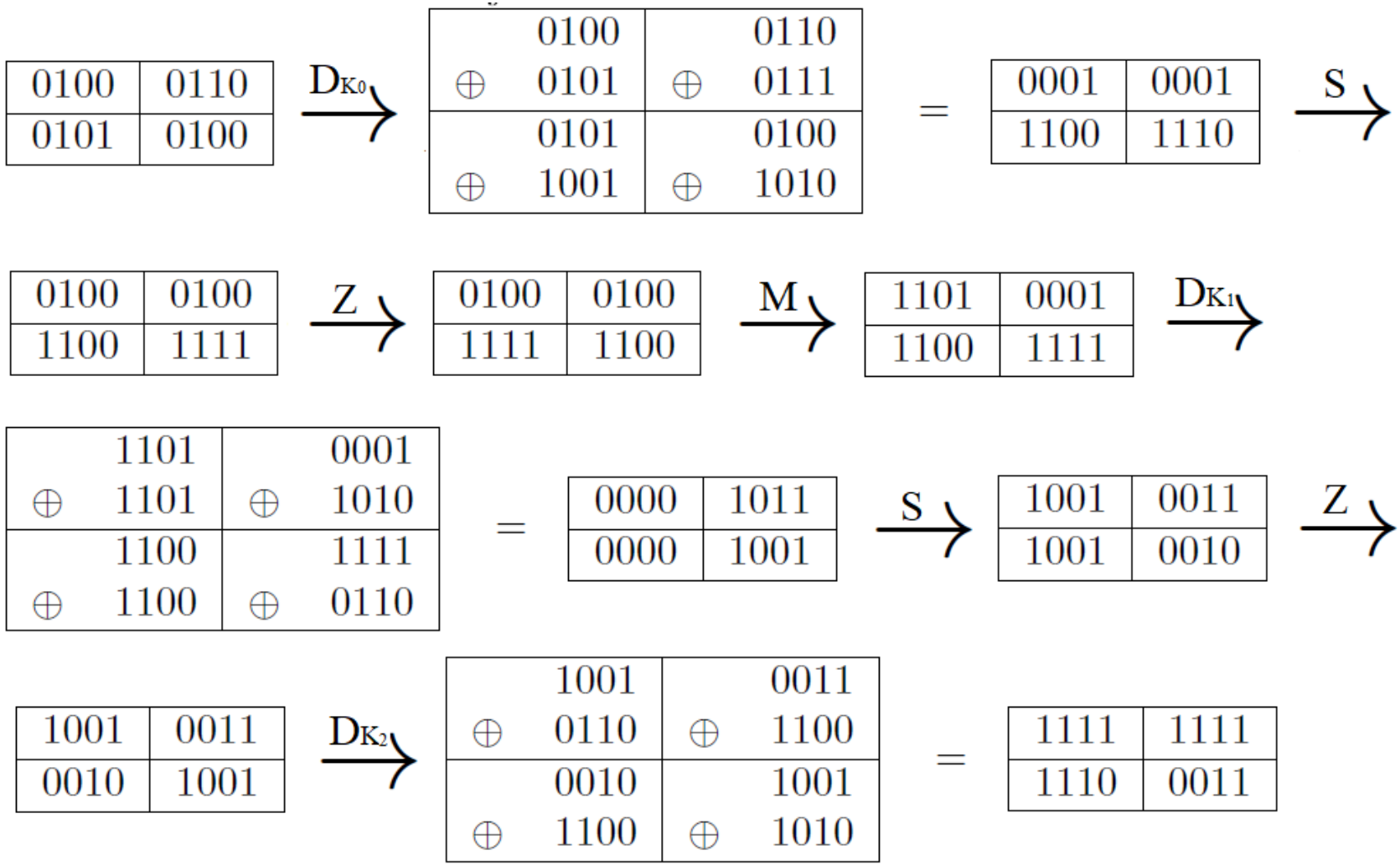
- M трансформише сваку од колона $\boxed{\begin{array}{c} N_j \\ \hline N_k \end{array}}$ на следећи начин:
  - користи се прстен $\mathbb{F}_{16}[y] \,/\, \left(\left(y^2+1\right)\mathbb{F}_{16}[y]\right)$, или интуитивније записано $\mathbb{F}_{16}[i]$, $i^2 = -1$ $(= 1$ у $\mathbb{F}_{16})$
  - колона се поистовећује са $N_j i + N_k$, затим се помножи са $x^2 i + 1$, резултат се запише у облику $Ai + B$, $A, B \in \mathbb{F}_{16}$, и колона $\boxed{\begin{array}{c} A \\ \hline B \end{array}}$ је резултат трансформације M
  - Пример: $M\left(\boxed{\begin{array}{c} 1010 \\ \hline 1001 \end{array}}\right) = \left(\left(x^3+x\right)i + \left(x^3+1\right)\right)\left(x^2 i + 1\right)$

    $= \cdots = x^3 i + \left(x^2 + x + 1\right) = \boxed{\begin{array}{c} 1000 \\ \hline 0111 \end{array}}$
- У композицији SAES имамо само 3 криптовања D_{K_0}, D_{K_1} и D_{K_2}, остале функције не зависе од параметара (тј. увек користе једне исте кључеве)

- M трансформише сваку од колона $\boxed{\begin{array}{c} N_j \\ \hline N_k \end{array}}$ на следећи начин:
  - користи се прстен $\mathbb{F}_{16}[y] / \left(\left(y^2 + 1 \right) \mathbb{F}_{16}[y] \right)$, или интуитивније записано $\mathbb{F}_{16}[i]$, $i^2 = -1$ $(= 1$ у $\mathbb{F}_{16})$
  - колона се поистовећује са $N_j i + N_k$, затим се помножи са $x^2 i + 1$, резултат се запише у облику $Ai + B$, $A, B \in \mathbb{F}_{16}$, и колона $\boxed{\begin{array}{c} A \\ \hline B \end{array}}$ је резултат трансформације M
  - Пример: $M \left(\boxed{\begin{array}{c} 1010 \\ \hline 1001 \end{array}} \right) = \left(\left(x^3 + x \right) i + \left(x^3 + 1 \right) \right) \left(x^2 i + 1 \right)$

    $= \cdots = x^3 i + \left(x^2 + x + 1 \right) = \boxed{\begin{array}{c} 1000 \\ \hline 0111 \end{array}}$
- У композицији SAES имамо само 3 криптовања D_{K_0}, D_{K_1} и D_{K_2}, остале функције не зависе од параметара (тј. увек користе једне исте кључеве)
  - $M \circ Z \circ S$ треба да имитира произвољну трансформацију 16 битова и служи да предупреди $D_{K_1} \circ D_{K_0} = D_{K_0 + K_1}$

Пример: Кључевима $K_0 = 0101\ 1001\ 0111\ 1010$,
$K_1 = 1101\ 1100\ 1010\ 0110$ и $K_2 = 0110\ 1100\ 1100\ 1010$ из претх. примера криптовати поруку $'Ed' = 01000101\ 01100100$



шифрат је $11111110\ 11110011$

Декриптовање SAES

- Свака од 8 функција криптовања из дефиниције SAES-а има инверз па ће функција декриптовања бити

$$D_{K_0}^{-1} \circ S^{-1} \circ Z^{-1} \circ M^{-1} \circ D_{K_1}^{-1} \circ S^{-1} \circ Z^{-1} \circ D_{K_2}^{-1}$$

  - притом је $D_{K_j}^{-1} = D_{K_j}$ и $Z^{-1} = Z$ (инволуције)

Декриптовање SAES

- Свака од 8 функција криптовања из дефиниције SAES-а има инверз па ће функција декриптовања бити

$$D_{K_0}^{-1} \circ S^{-1} \circ Z^{-1} \circ M^{-1} \circ D_{K_1}^{-1} \circ S^{-1} \circ Z^{-1} \circ D_{K_2}^{-1}$$

  - притом је $D_{K_j}^{-1} = D_{K_j}$ и $Z^{-1} = Z$ (инволуције)
  - $S^{-1} = S_1^{-1} \circ S_2^{-1}$ и $S_1^{-1} = S_1$
    - $S_2^{-1}\left(b_3 b_2 b_1 b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^2 + x + 1\right)\left(b_3 x^3 + b_2 x^2 + b_1 x + b_0\right) + \left(x^3 + x^2\right)$

Декриптовање SAES

- Свака од 8 функција криптовања из дефиниције SAES-а има инверз па ће функција декриптовања бити

$$D_{K_0}^{-1} \circ S^{-1} \circ Z^{-1} \circ M^{-1} \circ D_{K_1}^{-1} \circ S^{-1} \circ Z^{-1} \circ D_{K_2}^{-1}$$

  - притом је $D_{K_j}^{-1} = D_{K_j}$ и $Z^{-1} = Z$ (инволуције)
  - $S^{-1} = S_1^{-1} \circ S_2^{-1}$ и $S_1^{-1} = S_1$
    - $S_2^{-1}(b_3 b_2 b_1 b_0)$ ће бити нибл који даје афино пресликавање $\left(x^2 + x + 1\right)\left(b_3 x^3 + b_2 x^2 + b_1 x + b_0\right) + \left(x^3 + x^2\right)$
    - слично се одређује M^{-1}

Декриптовање SAES

- Свака од 8 функција криптовања из дефиниције SAES-а има инверз па ће функција декриптовања бити

$$D_{K_0}^{-1} \circ S^{-1} \circ Z^{-1} \circ M^{-1} \circ D_{K_1}^{-1} \circ S^{-1} \circ Z^{-1} \circ D_{K_2}^{-1}$$

  - притом је $D_{K_j}^{-1} = D_{K_j}$ и $Z^{-1} = Z$ (инволуције)
  - $S^{-1} = S_1^{-1} \circ S_2^{-1}$ и $S_1^{-1} = S_1$
    - $S_2^{-1}\left(b_3 b_2 b_1 b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^2 + x + 1\right)\left(b_3 x^3 + b_2 x^2 + b_1 x + b_0\right) + \left(x^3 + x^2\right)$
    - слично се одређује M^{-1}
  - Важно: свака (од 8) функција је инверз сама себи (евентуално са другачијим кључем)

Декриптовање SAES

- Свака од 8 функција криптовања из дефиниције SAES-а има инверз па ће функција декриптовања бити

$$D_{K_0}^{-1} \circ S^{-1} \circ Z^{-1} \circ M^{-1} \circ D_{K_1}^{-1} \circ S^{-1} \circ Z^{-1} \circ D_{K_2}^{-1}$$

  - притом је $D_{K_j}^{-1} = D_{K_j}$ и $Z^{-1} = Z$ (инволуције)
  - $S^{-1} = S_1^{-1} \circ S_2^{-1}$ и $S_1^{-1} = S_1$
    - $S_2^{-1}\left(b_3 b_2 b_1 b_0\right)$ ће бити нибл који даје афино пресликавање $\left(x^2 + x + 1\right)\left(b_3 x^3 + b_2 x^2 + b_1 x + b_0\right) + \left(x^3 + x^2\right)$
    - слично се одређује M^{-1}
  - Важно: свака (од 8) функција је инверз сама себи (евентуално са другачијим кључем)
  - Може се постићи и исти редослед јер многе (али не све) наведене функције комутирају

Криптосистем AES је отпоран на све познате нападе. На сигурност повољно утичу:

- Потпуна дифузија - сваки бит почетног кључа K_0, утиче на све битове нових кључева K_1 и K_2, а тиме и на све битове шифрата. Примена трансформација Z и M такође повећава дифузију

Криптосистем AES је отпоран на све познате нападе. На сигурност повољно утичу:

- Потпуна дифузија - сваки бит почетног кључа K_0, утиче на све битове нових кључева K_1 и K_2, а тиме и на све битове шифрата. Примена трансформација Z и M такође повећава дифузију
- Нелинеарност - нису сва пресликавања афина нпр. имамо узимање инверза. Уколико Цица покуша да ради криптоанализу добиће нелинеарни систем једначина, који не може да реши тј. направи алгоритам за решавање

Криптосистем AES је отпоран на све познате нападе. На сигурност повољно утичу:

- Потпуна дифузија - сваки бит почетног кључа K_0, утиче на све битове нових кључева K_1 и K_2, а тиме и на све битове шифрата. Примена трансформација Z и M такође повећава дифузију
- Нелинеарност - нису сва пресликавања афина нпр. имамо узимање инверза. Уколико Цица покуша да ради криптоанализу добиће нелинеарни систем једначина, који не може да реши тј. направи алгоритам за решавање
- Шифровање се врши више пута - теже је криптоанализирати шифровање шифрата од шифровања отвореног текста (где се ефективно појављује четвртина ASCII симбола и има бројне друге правилности)

- Ефикасност:
  - не захтева велики меморијски простор и све операције се брзо извршавају

- Ефикасност:
  - не захтева велики меморијски простор и све операције се брзо извршавају
  - многи кораци се понављају (код комплетног SAES-а још више) и криптовање и декриптовање су исте функције. Понављање је посебно значајно ако се све реализује на чипу

- Ефикасност:
  - не захтева велики меморијски простор и све операције се брзо извршавају
  - многи кораци се понављају (код комплетног SAES-а још више) и криптовање и декриптовање су исте функције. Понављање је посебно значајно ако се све реализује на чипу
  - многе операције се могу извршавати паралелно нпр. примена S на појединачне ниблове

- Ефикасност:
  - не захтева велики меморијски простор и све операције се брзо извршавају
  - многи кораци се понављају (код комплетног SAES-а још више) и криптовање и декриптовање су исте функције. Понављање је посебно значајно ако се све реализује на чипу
  - многе операције се могу извршавати паралелно нпр. примена S на појединачне ниблове
- Због једноставности криптосистема много људи покушава криптоанализу, неуспеси повећавају поверење у шифру

- Ефикасност:
  - не захтева велики меморијски простор и све операције се брзо извршавају
  - многи кораци се понављају (код комплетног SAES-а још више) и криптовање и декриптовање су исте функције. Понављање је посебно значајно ако се све реализује на чипу
  - многе операције се могу извршавати паралелно нпр. примена S на појединачне ниблове
- Због једноставности криптосистема много људи покушава криптоанализу, неуспеси повећавају поверење у шифру
- Све константе у алгоритмима су биране тако да се минимизује израчунавање (гледано статистички)

Начини примене AES-а (или произвољног блоковског криптосистема)

(P_j и C_j су i-ти блок отвореног текста и шифрата, редом)

- Директна примена $C_j = AES(P_j)$
  - Главни недостатак: последњи блок се (по потреби) допуњава са неколико празних симбола - добра полазна тачка за криптоанализу

Начини примене AES-а (или произвољног блоковског криптосистема)

(P_j и C_j су i-ти блок отвореног текста и шифрата, редом)

- Директна примена $C_j = AES\left(P_j\right)$
  - Главни недостатак: последњи блок се (по потреби) допуњава са неколико празних симбола - добра полазна тачка за криптоанализу
- (најчешћа примена) $C_j = AES\left(C_{j-1} + P_j\right)$, при чему се C_{-1} поставља на нулу или неку други вредност коју Алиса и Бобан договоре

Начини примене AES-а (или произвољног блоковског криптосистема)

(P_j и C_j су i-ти блок отвореног текста и шифрата, редом)

- Директна примена $C_j = AES\left(P_j\right)$
  - Главни недостатак: последњи блок се (по потреби) допуњава са неколико празних симбола - добра полазна тачка за криптоанализу
- (најчешћа примена) $C_j = AES\left(C_{j-1} + P_j\right)$, при чему се C_{-1} поставља на нулу или неку други вредност коју Алиса и Бобан договоре
- $C_j = AES\left(C_{j-1}\right) + P_j$, и C_{-1} као у претх.
  - не шифрује се блок отвореног текста P_j већ се шифрује претходни шифрат C_{j-1} и сабира са P_j.
  - задњи блок: можемо скратити $AES\left(C_{j-1}\right)$ уместо да продужавамо P_j.

Начини примене AES-а (или произвољног блоковског криптосистема)

(P_j и C_j су i-ти блок отвореног текста и шифрата, редом)

- Директна примена $C_j = AES(P_j)$
  - Главни недостатак: последњи блок се (по потреби) допуњава са неколико празних симбола - добра полазна тачка за криптоанализу
- (најчешћа примена) $C_j = AES(C_{j-1} + P_j)$, при чему се C_{-1} поставља на нулу или неку други вредност коју Алиса и Бобан договоре
- $C_j = AES(C_{j-1}) + P_j$, и C_{-1} као у претх.
  - не шифрује се блок отвореног текста P_j већ се шифрује претходни шифрат C_{j-1} и сабира са P_j.
  - задњи блок: можемо скратити $AES(C_{j-1})$ уместо да продужавамо P_j.
- аналог RC4 који користи AES уместо генератора псеудослучајних бројева:
  - почетни кључ K_0 се прошири до $K_0K_1K_2\ldots$ тд. $K_j = AES(K_{j-1})$
  - примени се OTP са проширеним кључем

„Сусрет на пола пута“

- је најпознатији напад на блоковске криптосистеме, објашњава понављање корака у AES-у

„Сусрет на пола пута“

- је најпознатији напад на блоковске криптосистеме, објашњава понављање корака у AES-у
- $n =$ дужина блока, f_K и f_K^{-1} функције криптовања и декриптовања кључем K
- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C

„Сусрет на пола пута“

- је најпознатији напад на блоковске криптосистеме, објашњава понављање корака у AES-у
- $n =$ дужина блока, f_K и f_K^{-1} функције криптовања и декриптовања кључем K
- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C
- Цица може да уради потпуну претрагу - испроба свих 2^n кључева и пронађе онај за који је $f_K(P) = C$
  - ако има више одговарајућих провери на следећем пару (P, C)
  - потребно 2^n покушаја, код AES-а је то 2^{128}, што је изводљиво

„Сусрет на пола пута“

- је најпознатији напад на блоковске криптосистеме, објашњава понављање корака у AES-у
- $n =$ дужина блока, f_K и f_K^{-1} функције криптовања и декриптовања кључем K
- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C
- Цица може да уради потпуну претрагу - испроба свих 2^n кључева и пронађе онај за који је $f_K(P) = C$
  - ако има више одговарајућих провери на следећем пару (P, C)
  - потребно 2^n покушаја, код AES-а је то 2^{128}, што је изводљиво
- Овај напад ће показати да ни двоструко криптовање (различитим кључевима) није сигурније

„Сусрет на пола пута“

- је најпознатији напад на блоковске криптосистеме, објашњава понављање корака у AES-у
- $n =$ дужина блока, f_K и f_K^{-1} функције криптовања и декриптовања кључем K
- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C
- Цица може да уради потпуну претрагу - испроба свих 2^n кључева и пронађе онај за који је $f_K(P) = C$
  - ако има више одговарајућих провери на следећем пару (P, C)
  - потребно 2^n покушаја, код AES-а је то 2^{128}, што је изводљиво
- Овај напад ће показати да ни двоструко криптовање (различитим кључевима) није сигурније
- Зато SAES има три понављања (и три кључа K_0, K_1, K_2), а комплетан AES осам понављања

„Сусрет на пола пута“

- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C и зна да је два пута примењен криптосистем f...

„Сусрет на пола пута“

- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C и зна да је два пута примењен криптосистем f...
- Цица криптује $f_{K_1}(P)$ за све могуће кључеве K_1 и чува добијене шифрате у сортираној листи

„Сусрет на пола пута“

- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C и зна да је два пута примењен криптосистем f...
- Цица криптује $f_{K_1}(P)$ за све могуће кључеве K_1 и чува добијене шифрате у сортираној листи
- Цица декриптује $f_{K_2}^{-1}(C)$ за све могуће кључеве K_2 и чува добијене шифрате у сортираној листи

„Сусрет на пола пута“

- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C и зна да је два пута примењен криптосистем f...
- Цица криптује $f_{K_1}(P)$ за све могуће кључеве K_1 и чува добијене шифрате у сортираној листи
- Цица декриптује $f_{K_2}^{-1}(C)$ за све могуће кључеве K_2 и чува добијене шифрате у сортираној листи
- Проналази поклапање у листи $f_{K_1}(P) = f_{K_2}^{-1}(C)$ и тако долази до кључева K_1, K_2
  - Сортираност омогућава пролаз кроз обе листе у $O\left(2^n\right)$ корака

„Сусрет на пола пута“

- претпостављамо да Цица има један пар (или више њих) отворени текст P и шифрат C и зна да је два пута примењен криптосистем f...
- Цица криптује $f_{K_1}(P)$ за све могуће кључеве K_1 и чува добијене шифрате у сортираној листи
- Цица декриптује $f_{K_2}^{-1}(C)$ за све могуће кључеве K_2 и чува добијене шифрате у сортираној листи
- Проналази поклапање у листи $f_{K_1}(P) = f_{K_2}^{-1}(C)$ и тако долази до кључева K_1, K_2
  - Сортираност омогућава пролаз кроз обе листе у $O\left(2^n\right)$ корака
- Ако користи алгоритам за брзо сортирање временска сложеност је $O\left(n2^n\right)$ (пута временска сложеност функције (де)криптовања)
  - није значајно дуже од напада на једноструку шифру!