DIFERENCIJALNA KRIPTOANALIZA

Oznake :

$\Delta(B_j') = \{(B_j, B_j \oplus B_j') : B_j \in Z_2^6\}$;

$B_j \oplus B_j'$ **input XOR**

$S_j(B_j) \oplus S_j(B_j')$ **output XOR**

$B' = (1, 1, 0, 1, 0, 0)$, $\Delta(B')$ je sljedeci skup :

```
{{{0, 0, 0, 0, 0, 0}, {1, 1, 0, 1, 0, 0}}, {{0, 0, 0, 0, 0, 1}, {1, 1, 0, 1, 0, 1}},
 {{0, 0, 0, 0, 1, 0}, {1, 1, 0, 1, 1, 0}}, {{0, 0, 0, 0, 1, 1}, {1, 1, 0, 1, 1, 1}},
 {{0, 0, 0, 1, 0, 0}, {1, 1, 0, 0, 0, 0}}, {{0, 0, 0, 1, 0, 1}, {1, 1, 0, 0, 0, 1}},
 {{0, 0, 0, 1, 1, 0}, {1, 1, 0, 0, 1, 0}}, {{0, 0, 0, 1, 1, 1}, {1, 1, 0, 0, 1, 1}},
 {{0, 0, 1, 0, 0, 0}, {1, 1, 1, 1, 0, 0}}, {{0, 0, 1, 0, 0, 1}, {1, 1, 1, 1, 0, 1}},
 {{0, 0, 1, 0, 1, 0}, {1, 1, 1, 1, 1, 0}}, {{0, 0, 1, 0, 1, 1}, {1, 1, 1, 1, 1, 1}},
 {{0, 0, 1, 1, 0, 0}, {1, 1, 1, 0, 0, 0}}, {{0, 0, 1, 1, 0, 1}, {1, 1, 1, 0, 0, 1}},
 {{0, 0, 1, 1, 1, 0}, {1, 1, 1, 0, 1, 0}}, {{0, 0, 1, 1, 1, 1}, {1, 1, 1, 0, 1, 1}},
 {{0, 1, 0, 0, 0, 0}, {1, 0, 0, 1, 0, 0}}, {{0, 1, 0, 0, 0, 1}, {1, 0, 0, 1, 0, 1}},
 {{0, 1, 0, 0, 1, 0}, {1, 0, 0, 1, 1, 0}}, {{0, 1, 0, 0, 1, 1}, {1, 0, 0, 1, 1, 1}},
 {{0, 1, 0, 1, 0, 0}, {1, 0, 0, 0, 0, 0}}, {{0, 1, 0, 1, 0, 1}, {1, 0, 0, 0, 0, 1}},
 {{0, 1, 0, 1, 1, 0}, {1, 0, 0, 0, 1, 0}}, {{0, 1, 0, 1, 1, 1}, {1, 0, 0, 0, 1, 1}},
 {{0, 1, 1, 0, 0, 0}, {1, 0, 1, 1, 0, 0}}, {{0, 1, 1, 0, 0, 1}, {1, 0, 1, 1, 0, 1}},
 {{0, 1, 1, 0, 1, 0}, {1, 0, 1, 1, 1, 0}}, {{0, 1, 1, 0, 1, 1}, {1, 0, 1, 1, 1, 1}},
 {{0, 1, 1, 1, 0, 0}, {1, 0, 1, 0, 0, 0}}, {{0, 1, 1, 1, 0, 1}, {1, 0, 1, 0, 0, 1}},
 {{0, 1, 1, 1, 1, 0}, {1, 0, 1, 0, 1, 0}}, {{0, 1, 1, 1, 1, 1}, {1, 0, 1, 0, 1, 1}},
 {{1, 0, 0, 0, 0, 0}, {0, 1, 0, 1, 0, 0}}, {{1, 0, 0, 0, 0, 1}, {0, 1, 0, 1, 0, 1}},
 {{1, 0, 0, 0, 1, 0}, {0, 1, 0, 1, 1, 0}}, {{1, 0, 0, 0, 1, 1}, {0, 1, 0, 1, 1, 1}},
 {{1, 0, 0, 1, 0, 0}, {0, 1, 0, 0, 0, 0}}, {{1, 0, 0, 1, 0, 1}, {0, 1, 0, 0, 0, 1}},
 {{1, 0, 0, 1, 1, 0}, {0, 1, 0, 0, 1, 0}}, {{1, 0, 0, 1, 1, 1}, {0, 1, 0, 0, 1, 1}},
 {{1, 0, 1, 0, 0, 0}, {0, 1, 1, 1, 0, 0}}, {{1, 0, 1, 0, 0, 1}, {0, 1, 1, 1, 0, 1}},
 {{1, 0, 1, 0, 1, 0}, {0, 1, 1, 1, 1, 0}}, {{1, 0, 1, 0, 1, 1}, {0, 1, 1, 1, 1, 1}},
 {{1, 0, 1, 1, 0, 0}, {0, 1, 1, 0, 0, 0}}, {{1, 0, 1, 1, 0, 1}, {0, 1, 1, 0, 0, 1}},
 {{1, 0, 1, 1, 1, 0}, {0, 1, 1, 0, 1, 0}}, {{1, 0, 1, 1, 1, 1}, {0, 1, 1, 0, 1, 1}},
 {{1, 1, 0, 0, 0, 0}, {0, 0, 0, 1, 0, 0}}, {{1, 1, 0, 0, 0, 1}, {0, 0, 0, 1, 0, 1}},
 {{1, 1, 0, 0, 1, 0}, {0, 0, 0, 1, 1, 0}}, {{1, 1, 0, 0, 1, 1}, {0, 0, 0, 1, 1, 1}},
 {{1, 1, 0, 1, 0, 0}, {0, 0, 0, 0, 0, 0}}, {{1, 1, 0, 1, 0, 1}, {0, 0, 0, 0, 0, 1}},
 {{1, 1, 0, 1, 1, 0}, {0, 0, 0, 0, 1, 0}}, {{1, 1, 0, 1, 1, 1}, {0, 0, 0, 0, 1, 1}},
 {{1, 1, 1, 0, 0, 0}, {0, 0, 1, 1, 0, 0}}, {{1, 1, 1, 0, 0, 1}, {0, 0, 1, 1, 0, 1}},
 {{1, 1, 1, 0, 1, 0}, {0, 0, 1, 1, 1, 0}}, {{1, 1, 1, 0, 1, 1}, {0, 0, 1, 1, 1, 1}},
 {{1, 1, 1, 1, 0, 0}, {0, 0, 1, 0, 0, 0}}, {{1, 1, 1, 1, 0, 1}, {0, 0, 1, 0, 0, 1}},
 {{1, 1, 1, 1, 1, 0}, {0, 0, 1, 0, 1, 0}}, {{1, 1, 1, 1, 1, 1}, {0, 0, 1, 0, 1, 1}}}
```

Racunanje distribucije mogucih output XOR –

ova $S_j(B_j) \oplus S_j(B_j \oplus B_j')$ za sve elemente iz $\Delta(B_j') = \{(B_j, B_j \oplus B_j') : B_j \in Z_2^6\}$;

$S_j(B_j) \oplus S_j(B_j \oplus B_j')$ je niz duljine 4 bita –– > zapisat cemo kao broj iz {0, 1, .., 15}

Oznake :

$IN_j(B_j', C_j') = \{B_j \in Z_2^6 : S_j(B_j) \oplus S_j(B_j \oplus B_j') = C_j'\}$ (distribucije INput XOR – ova)

$N_j(B_j', C_j') =$ card $(IN_j(B_j', C_j'))$ (frekvencije INput XOR – ova)

(indeks "j" se odnosi na kutiju S_j)

B′ = (1, 1, 0, 1, 0, 0),
u tablicu su dani $IN_1(B', C')$ i $N_1(B', C')$ za sve moguce output XOR – ove $C' \in \{0, 1, .., 15\}$

Out[153]=

C′	$IN_1(B',C')$	$N_1(B',C')$
0	{}	0
1	{{0, 0, 0, 0, 1, 1}, {0, 0, 1, 1, 1, 1}, {0, 1, 1, 1, 1, 0}, {0, 1, 1, 1, 1, 1}, {1, 0, 1, 0, 1, 0}, {1, 0, 1, 0, 1, 1}, {1, 1, 0, 1, 1, 1}, {1, 1, 1, 0, 1, 1}}	8
2	{{0, 0, 0, 1, 0, 0}, {0, 0, 0, 1, 0, 1}, {0, 0, 1, 1, 1, 0}, {0, 1, 0, 0, 0, 1}, {0, 1, 0, 0, 1, 0}, {0, 1, 0, 1, 0, 0}, {0, 1, 1, 0, 1, 0}, {0, 1, 1, 0, 1, 1}, {1, 0, 0, 0, 0, 0}, {1, 0, 0, 1, 0, 1}, {1, 0, 0, 1, 1, 0}, {1, 0, 1, 1, 1, 0}, {1, 0, 1, 1, 1, 1}, {1, 1, 0, 0, 0, 0}, {1, 1, 0, 0, 0, 1}, {1, 1, 1, 0, 1, 0}}	16
3	{{0, 0, 0, 0, 0, 1}, {0, 0, 0, 0, 1, 0}, {0, 1, 0, 1, 0, 1}, {1, 0, 0, 0, 0, 1}, {1, 1, 0, 1, 0, 1}, {1, 1, 0, 1, 1, 0}}	6
4	{{0, 1, 0, 0, 1, 1}, {1, 0, 0, 1, 1, 1}}	2
5	{}	0
6	{}	0
7	{{0, 0, 0, 0, 0, 0}, {0, 0, 1, 0, 0, 0}, {0, 0, 1, 1, 0, 1}, {0, 1, 0, 1, 1, 1}, {0, 1, 1, 0, 0, 0}, {0, 1, 1, 1, 0, 1}, {1, 0, 0, 0, 1, 1}, {1, 0, 1, 0, 0, 1}, {1, 0, 1, 1, 0, 0}, {1, 1, 0, 1, 0, 0}, {1, 1, 1, 0, 0, 1}, {1, 1, 1, 1, 0, 0}}	12
8	{{0, 0, 1, 0, 0, 1}, {0, 0, 1, 1, 0, 0}, {0, 1, 1, 0, 0, 1}, {1, 0, 1, 1, 0, 1}, {1, 1, 1, 0, 0, 0}, {1, 1, 1, 1, 0, 1}}	6
9	{}	0
10	{}	0
11	{}	0
12	{}	0
13	{{0, 0, 0, 1, 1, 0}, {0, 1, 0, 0, 0, 0}, {0, 1, 0, 1, 1, 0}, {0, 1, 1, 1, 0, 0}, {1, 0, 0, 0, 1, 0}, {1, 0, 0, 1, 0, 0}, {1, 0, 1, 0, 0, 0}, {1, 1, 0, 0, 1, 0}}	8
14	{}	0
15	{{0, 0, 0, 1, 1, 1}, {0, 0, 1, 0, 1, 0}, {0, 0, 1, 0, 1, 1}, {1, 1, 0, 0, 1, 1}, {1, 1, 1, 1, 1, 0}, {1, 1, 1, 1, 1, 1}}	6

Racunanje skupa

$$test_j\left(E_j, E_j^*, C_j'\right) = \left\{B_j \oplus E_j : B_j \in IN_j\left(E_j \oplus E_j^*, C_j'\right)\right\}$$

gdje je $E_j, E_j^* \in Z_2^6$ i $C_j' \in Z_2^4$.

Racunanje skupa

$$test_1(E = (0, 0, 0, 1, 0, 1), E^* = (1, 1, 0, 0, 0, 1), (0, 0, 0, 1) = 1)$$

$B' = (0, 0, 0, 1, 0, 1) \oplus (1, 1, 0, 0, 0, 1) = (1, 1, 0, 1, 0, 0)$
$IN_1(B', 1) = \{(0, 0, 0, 0, 1, 1), (0, 0, 1, 1, 1, 1), (0, 1, 1, 1, 1, 0), (0, 1, 1, 1, 1, 1), (1, 0, 1, 0, 1, 0), (1, 0, 1, 0, 1, 1), (1, 1, 0, 1, 1, 1), (1, 1, 1, 0, 1, 1)\}$
$test_1(E, E^*, 1) = E \oplus IN_1(B', 1) =$
$=$
$\{(0, 0, 0, 1, 1, 0), (0, 0, 1, 0, 1, 0), (0, 1, 1, 0, 1, 1), (0, 1, 1, 0, 1, 0), (1, 0, 1, 1, 1, 1), (1, 0, 1, 1, 1, 0), (1, 1, 0, 0, 1, 0), (1, 1, 1, 1, 1, 0)\}$