Завдання PRESENT

Толстопятий Андрій, ТТП-31, 15 номер у списку

Умова: $x = (\underbrace{0\ldots0}_{59\text{ нулів}}10100)$ $K_1 = (\underbrace{0\ldots0}_{60\text{ нулів}}1010)$ $K_2 = (\underbrace{0\ldots0}_{60\text{ нулів}}1011)$

Розв'язок:

I раунд

1) $x \oplus k_1 = (\underbrace{0\ldots0}_{59\text{ нулів}}11110)$

2) ~~$S(0\ldots0)$~~ $S(x \oplus k_1) = \underbrace{S(0000)\ldots S(0000)}_{14} S(0001) S(1110) =$

$= \underbrace{S(0)\ldots S(0)}_{14} S(1) S(E) = \underbrace{(c)\ldots(c)}_{14}(5)(1) = \underbrace{(1100)\ldots(1100)}_{14}(0101)(0001)$

3) $P(S(x \oplus k_1)) = P(1100110011001100110011001100110011001100110011001100110011001100\underline{0101}\underline{0001}) =$

$= (1111111111111001111111111111110000000000000000000000000011) = y$

II раунд

1) $y \oplus K_2 = (\underbrace{1\ldots1}_{14}00\underbrace{1\ldots1}_{14}10\underbrace{0\ldots0}_{28}1000)$

2) $S(y \oplus k_2) = \underbrace{S(1111)\ldots S(1111)}_{3} S(1100) \underbrace{S(1111)\ldots S(1111)}_{3} S(1110) \underbrace{S(0000)\ldots S(0000)}_{7} S(1000) =$

$= \underbrace{S(F)\ldots S(F)}_{3} S(C) \underbrace{S(F)\ldots S(F)}_{3} S(E) \underbrace{S(0)\ldots S(0)}_{7} S(8) = \underbrace{(2)\ldots(2)}_{3} (4) \underbrace{(2)\ldots(2)}_{3} (1) \underbrace{(C)\ldots(C)}_{7} (3) =$

$= \underbrace{(0010)\ldots(0010)}_{3} (0100) \underbrace{(0010)\ldots(0010)}_{3} (0001) \underbrace{(1100)\ldots(1100)}_{7} (0011)$

3) $P(S(y \oplus k_2)) = P(001000100010010000100010001000111001100110011001100110011000011) =$

$= (00000000111111100001000011111111011101110000000010000000100000001)$

Відповіді на питання:

① Сутність мультирежимної криптографії полягає у забезпеченні компромісу між варіантом реалізації, швидкістю, безпекою, продуктивністю та енергоспоживанням на пристроях з обмеженими ресурсами.

Вони призначені для використання в пристроях, що мають обмежені обчислювальні потужності, пам'ять або час для виконання операцій. Головна мотивація досягти „практичного" рівня безпеки, використовуючи менший обсяг пам'яті, менші обчислювальні ресурси та менше енергоспоживання. Ці алгоритми вважаються стійкими за припущення, що зловмисник також має обмежені ресурси

② Авторами алгоритму є A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe, алгоритм був запропонований у 2007 році

③ Параметри алгоритму PRESENT:

1) Довжина блоку: 64 біти

2) Довжина ключа шифрування 80 бітів

3) Довжина раундового підключа: 64 біти

4) Кількість раундів: 31 повний раунд та один вкорочений 32-й раунд

5) З складові раунду: кожен повний раунд складається з ключового сумматора (побітове додавання з раундовим ключем), блоку підстановки (S-box) та бітової перестановки (P-layer)

6) Чи відрізняється останній раунд: Так. 32-й раунд складається лише з побітового додавання з раундовим ключем.