Жовтень 16, 2022

Алгоритм Shacal-1

Виконала:
студентка групи
ПМІ-43
Шувар Софія

Створення SHACAL-1

Створення: 2000р.

Опублікування: 2001 р.

Походить з: SHA-1, SHA-256

Сертифікація: NESSIE (SHACAL-2)

Хелена Хандшу

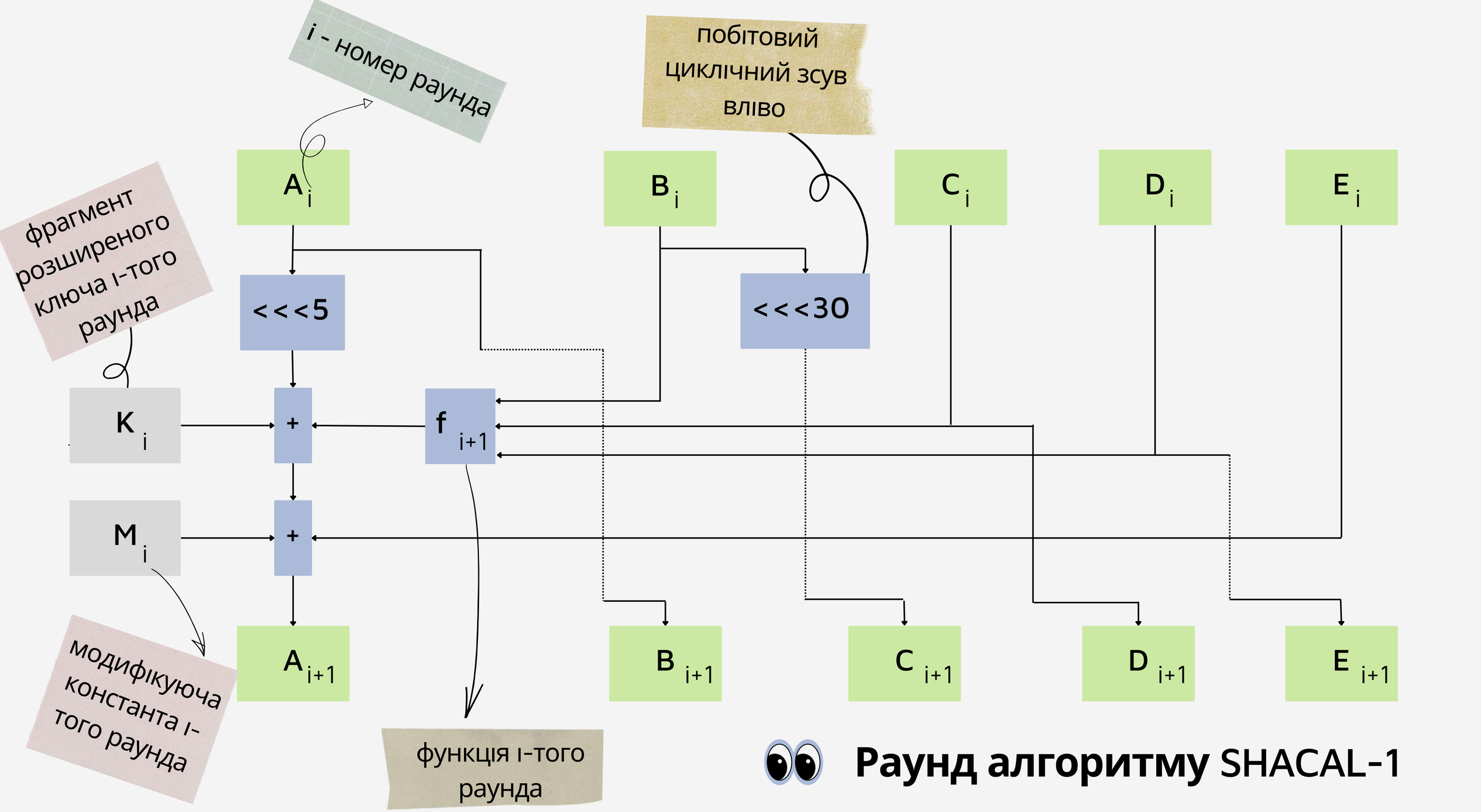
Давид Наккаш

Загальні відомості

Розмір ключа	128-512 **біт**	16-64 **символів**
Розмір блоку	160 **біт**	20 **символів**
Число раундів	80	

Шифрування

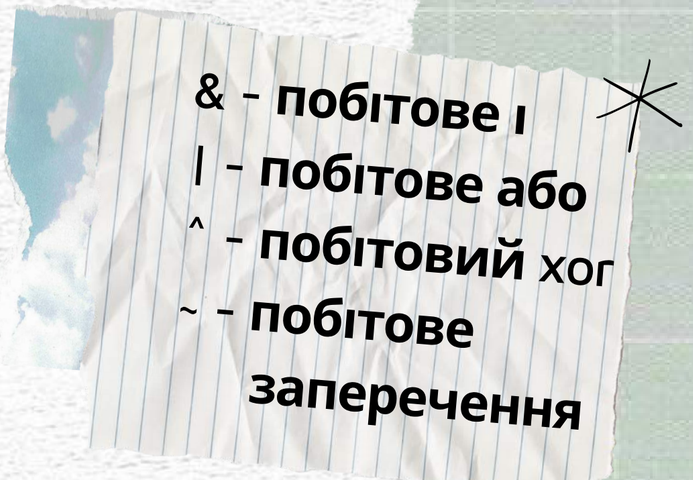
SHACAL-1



Раунд алгоритму SHACAL-1

Раунди	Значення константи
0 - 19	5A827999
20 - 39	6ED9EBA1
40 - 59	8F1BBCDC
60 - 70	CA62C1D6

Раунди	Значення константи
0 - 19	f(x, y, z) = (x & y) | (~x & z)
20 - 39	f(x, y, z) = x ^ y ^z
40 - 59	f(x, y, z) = (x ^ y) | (x ^ z) | (y ^ z)
60 - 70	f(x, y, z) = x ^ y ^z



Усі операції відбуваються на блоках довжини 32 біти

Розширення ключа

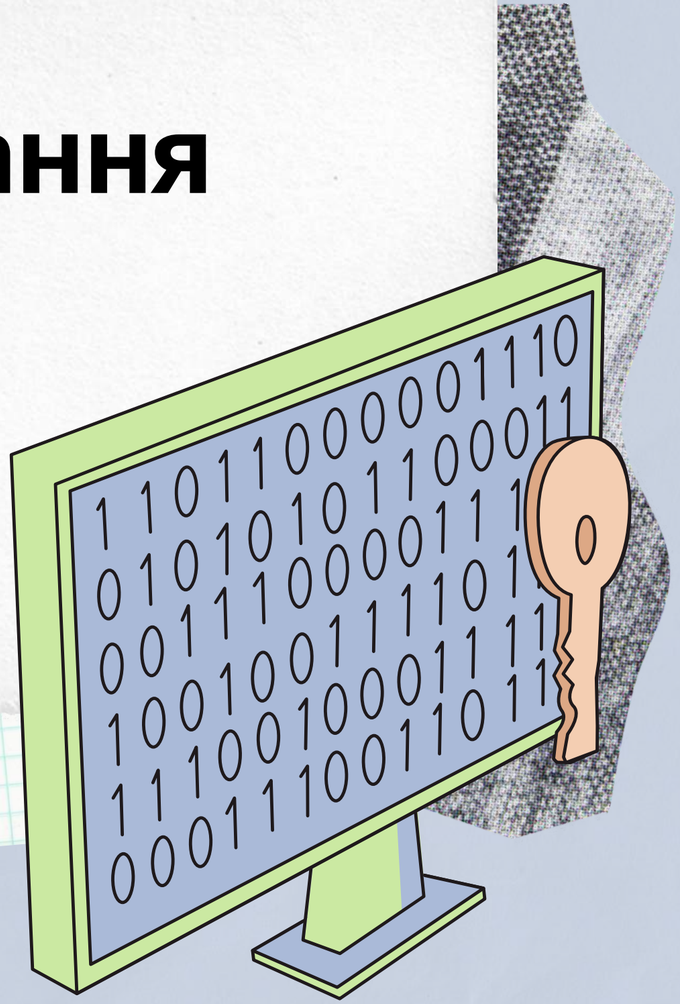
512-бітний вхідний ключ шифрування ділиться на 16 фрагментів по 32 біти - K0, K1...K15

Інші фрагменти розширеного ключа K16...K79 вираховуються з перших 16 фрагментів наступним чином:

$$K_i = (K_{i-3} \hat{} K_{i-8} \hat{} K_{i-14} \hat{} K_{i-16}) \cdot <<< 1$$

Розшифрування

SHACAL-1



Розшифрування

$$A_{i+1} = K_i + (A_i \lll 5) + f_i(B_i, C_i, D_i) + E_i + M_i$$

$$B_{i+1} = A_i$$

$$C_{i+1} = B_i \lll 30$$

$$D_{i+1} = C_i$$

$$E_{i+1} = D_i$$

$$X - Y = X + (2^{32} - 1 - Y) + 1 = X + \sim Y + 1$$

$$A_r = B_{r+1}$$

$$B_r = C_{r+1} \lll 2$$

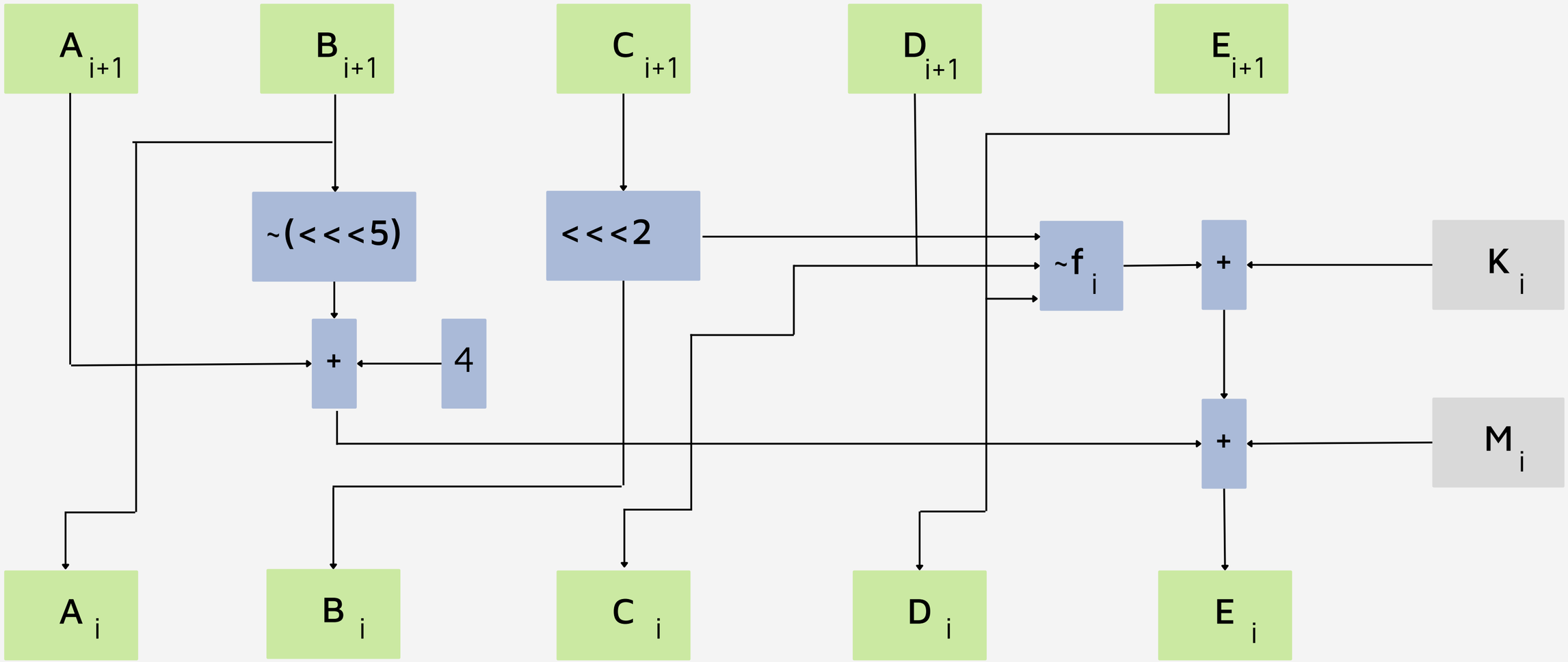
$$D_r = E_{r+1}$$

$$C_r = D_{r+1}$$

$$E_r = A_{r+1} - K_r - M_r - (A_r \lll 5) - f(B_r, C_r, D_r) =$$

$$= A_{r+1} + \sim K_r + \sim M_r + \sim (A_r \lll 5) + \sim f(B_r, C_r, D_r) + 4 =$$

$$= A_{r+1} + \sim K_r + \sim M_r + \sim (B_{r+1} \lll 5) + \sim f(C_{r+1} \lll 2, D_{r+1}, E_{r+1}) + 4$$



👀 **Раунд алгоритму дешифруванняSHACAL-1**

Висновок

Переваги SHACAL-1

- простота реалізації
- низькі вимоги до ресурсів
- висока швидкість