Kolokwium pierwsze

Mateusz Kroplewski

06.12.2022

1 Szyfrowanie blokowe

Szyfrowanie blokowe [1] traktuje poszczególne bloki tekstu jawnego jako odrębne całości i każdy z nich produkuje szyfrogram tej samej długości. Zazwyczaj używane są bloki o długości 64 lub 128 bitów. Podobnie jak w przypadku szyfru strumieniowego obaj uczestnicy komunikacji współdzielą ten sam klucz. Przy wykorzystaniu różnych trybów operacyjnych,za pomocą szyfru blokowego można osiągnąć efekty podobne do tych , jakie daje szyfrowanie strumieniowe.
Wiele wysiłku poświęcono zbadaniu właściwości szyfrów blokowych. Generalnie znajdują one wyraźnie większe zastosowanie niż szyfry strumieniowe: większość aplikacji sieciowych realizujących szyfrowanie symetryczne wykorzystuje właśnie szyfry blokowe.

1.1 Standard DES

Najbardziej rozpowszechnionym obecnie schematem szyfrowania jest DES (*Data Encryption Standard*) [2], przyjęty w 1977 roku przez Narodowe Biuro Standaryzacji USA (*National Bureau of Standards*), obecnie Narodowy Instytut Normalizacji i Technologi (NIST -*National Institute of Standards and Technology*) jako Federalny Standard Przetwarzania Informacji nr46 (FIST PUB 46). Sam algorytm szyfrowania określany jest jako *Data Encryption Algorithm*,w skrócie DEA. W standardzie DES dane wejściowe przetwarzane są w 64-bitowych blokach przy użyciu 56-bitowego klucza: algorytm transformuje 64-bitowe bloki tekstu jawnego na64-bitowe bloki szyfrogramu, te same kroki i przy użyciu tego samego klucza wykonywane są w ramach deszyfracji.

1.2 Szyfrowanie w standardzie DES

Tak jak w każdym schemacie szyfrowania informację wejściową stanowią dwa elementy: tekst jawny i klucz. Tekst jawny ma postać 64-bitowego bloku, długość klucza wynosi 56 bitów. Przetwarzanie tekstu jawnego odbywa się w trzech fazach. Pierwszą z nich stanowi **permutacja wstępna** (IP - *initial permutation*), w ramach której wejściowy blok 64-bitowy przekształcany jest do postaci permutowanego wejścia (*permuted input*). Faza druga stanowi ciąg **16 jednakowych rund**, z których każda obejmuje permutowanie i podstawianie, 32-bitowe połówki bloku stanowiącego wynik ostatniej rundy zamieniane są miejscami, po czym blok ten (zwany **wyjściem wstępnym**-*preoutput*) poddawany jest fazie trzeciej, czyli **permutacji stanowiącej odwrotność permutacji wstępnej**

Druga część odzwierciedla natomiast ciąg przekształceń, jakim poddawany jest 56-bitowy klucz. Pierwszym z tych przekształceń jest permutacja początkowa. Następnie w ramach każdej z 16 rund produkowane są *podklucze* K_i. Produkcja ta odbywa się w każdej rundzie dwuetapowo. W pierwszym etapie otrzymany podklucz poddawany jest operacji lewostronnego obrotu (o 1 lub 2 bity), wynik tego etapu przekazywany jest do następnej rundy; jest on jednocześnie permutowany (to drugi etap - wybór permutowany 2), dając w rezultacie klucz K_i. Permutacja wykonywana w drugim etapie jest identyczna dla każdej rundy, jednakże ze względu na powtarzaną (w pierwszym etapie) operację lewostronnego obrotu kolejne klucze K_i różnią się od siebie.

Przykład permutacji wstępnej w tabeli 1.2.

Tabela 1: Permutacja wstępna IP

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

1.3 Szczegóły jednej rundy

Oznaczmy przez L i R (odpowiednio) lewy i prawy półblok 64-biotowego bloku wejściowego; identycznie jak w klasycznej wersji szyfru Feistela są one traktowane oddzielnie, według formuły

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$$

Klucz rundy K_i ma rozmiar 48 bitów, wejściowy półblok R - 32 bity. Półblok ten jest wpierw rozszerzany do 48 bitów za pomocą złożenia permutacji i dublowania wybranych 16 bitów. Wynik tej operacji składany jest z kluczem K_i przez operację XOR. Wynik złożenia przetwarzany jest przez funkcję podstawieniową F zwracającą wartość 32-bitową, która następnie jest permutowana.

2 Ciasto jogurtowe z żurawiną

Fantastyczne, wilgotne, mięciutkie ciasto jogurtowe z żurawiną, suto polukrowane. Latem piekłam to ciasto z dodatkiem agrestu, teraz występuje w zimowej odsłonie. Ciasto długo utrzymuje świeżość a owoce żurawiny pasują tutaj jak żadne inne! [3]

Składniki na ciasto jogurtowe z żurawiną

1. 165g masła
2. 160 g drobnego cukru do wypieków
3. 8 g cukru wanilinowego lub 1 łyżeczka ekstraktu z wanilii
4. 3 duże jajka
5. 150 g jogurtu naturalnego lub greckiego
6. 270 g mąki pszennej
7. 2 łyżeczki proszku do pieczenia
8. 300 g żurawiny

Wszystkie składniki powinny być w temperaturze pokojowej.

W misie miksera umieścić masło i oba cukry (lub cukier i wanilię). Utrzeć do powstania jasnej i puszystej masy maślanej. Dodawać jajka, jedno po drugim, ucierając do całkowitego połączenia się składników po każdym dodaniu (ciasto na tym etapie może wyglądać na zwarzone, ale nie ma to wpływu na wypiek końcowy). Bezpośrednio do utartych składników przesiać mąkę pszenną i proszek do pieczenia oraz dodać jogurt. Wymieszać szpatułką tylko do połączenia się składników, nie dłużej. Dodać żurawinę i krótko wymieszać.

Formę o średnicy 25 cm wyłożyć papierem do pieczenia. Przełożyć do niej ciasto, wyrównać.

Ciasto jogurtowe z żurawiną piec w temperaturze 170°C, bez termoobiegu, przez około 50 minut lub dłużej, do tzw. suchego patyczka. Wyjąć i wystudzić w formie. Polukrować.

Waniliowy lukier

- 1 szklanka cukru pudru
- 2 - 3 łyżki wrzącej wody lub soku z cytryny
- 1 łyżeczka ekstraktu z wanilii

Wszystkie składniki umieścić miseczce i rozetrzeć grzbietem łyżki do otrzymania gęstego lukru (gęstość lukru regulować dodatkiem dodatkowego cukru pudru lub wody).

Literatura

[1] William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych* Helion, 2012, str.105

[2] William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych* Helion, 2012, str.115

[3] https://mojewypieki.com/przepis/ciasto-jogurtowe-z-zurawina