Kolokwium LaTeX

Ruslan Zhukotynskyi ISI 6

06.12.2022

1 Szyfr AES

Standard AES (*Advanced Encryption Standard*) opublikowany został przez NIST w 2001 roku. AES jest szyfrem blokowym, zaprojektowanym w celu zastąpienia szyfru DES jako przyjęty standard w różnorodnych zastosowaniach. W porównaniu z szyframi z kluczami publicznymi - jak RSA, AES (jak zresztą większość szyfrów symetrycznych) jest nieporównanie bardziej skomplikowany i nie da się wyjaśnić tak prosto jak wiele innych algorytmów kryptograficznych. Względna prostota tej wersji umożliwia ręczne wykonywanie szyfrowania i deszyfracji, dzięki czemu łatwiej można zrozumieć detale pełnego algorytmu AES [1].

1.1 Arytmetyka ciał skończonych

W Algorytmie AES wszystkie obliczenia wykonywane są na 8-bitowych bajtach, dodawanie, mnożenie i dzielenie wykonywane są w ciele skończonym GF(2^8). Mówiąc skrótowo, ciało to zbiór, w którym dodawanie, odejmowanie, mnożenie i dzielenie są działaniami wewnętrznymi: wynik dowolnej z tych operacji wykonanej na elementach zbioru również należy do tego zbioru. Dzielenie definiowane jest jako mnożenie przez element odwrotny: a/b oznacza to samo, co $a(b^{-1})$.

Wszystkie niemal algorytmy szyfrujące, zarówno te konwencjonalne, jak i te z kluczami publicznymi , obejmują obliczenia na liczbach całkowitych. Jeżeli jedną z operacji jest dzielenie, wymagana jest arytmetyka zdefiniowana nad ciałem: wykonalność dzielenia wiąże się bowiem z wymaganiem, by każdy nie zerowy element ciała posiadał odwrotność multiplikowaną. Ze względu na wygodę obliczeń oraz efektywności implementacji chcielibyśmy operować liczbami dającymi się zapisywać na ustalonej (n) liczbie bitów i jednocześnie w pełni wykorzystującymi zakres wartości (od 0 do 2^{n-1}) oferowanych przez tę liczbę bitów. Niestety, zbiór Z_{2^n} ze zwykłą arytmetyką modulo 2^n nie jest ciałem, ponieważ żadna liczba parzysta nie posiada w tej arytmetyce odwrotności multiplikowanej nie dla każdego elementu $b \in Z_{2^n}$ istnieje takie x, że $bx \bmod 2^n = 1$.

Możliwe jest jednak takie zdefiniowanie działań w zbiorze Z_{2^n} , by stał się ciałem GF(2^n). Rozpatrzymy zbiór S wielomianów stopnia nie wyższego niż n - 1 ze współczynnikami binarnymi (czyli pochodzącymi ze zbioru $\{0, 1\}$). Każdy z tych wielomianów ma postać

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = \sum_{i=0}^{n-1} a_i x^i$$

gdzie każde a^i ma wartość 0 albo 1. W zbiorze S istnieje wówczas dokładnie 2^n różnych wielomianów; dla n = 3 jest to 8 następujących wielomianów:

$$\begin{array}{llll} 0 & x & x^2 & x^2+x \\ 1 & x+1 & x^2+1 & x^2+x+1 \end{array}$$

Można sprawić, że zbiór S będzie ciałem skończonym, definiując odpowiednio operacje na jego elementach:

1. Operacje te opierać się muszą generalnie na tradycyjnych regułach arytmetyki wielomianowej, jednak z zastrzeżeniami wymienionymi w punktach 2. i 3.

2. Operacje na współczynnikach wielomianów wykonywane są modulo 2; dodawanie jest wówczas równoważne operacji XOR.

3. Gdy wynikiem mnożenia wielomianów jest wielomian $f(x)$ stopnia wyższego niż n - 1, należy wielomian ten zredukować modulo pewien nieredukowalny wielomian $m(x)$ stopnia n - czyli zamiast oryginalnego wielomianu $f(x)$ wziąć resztę $r(x)$ z jego dzielenia przez $m(x)$, oznaczoną $f(x) \bmod m(x)$. Wielomian nazywamy **nieredukowalnym**, jeżeli nie można go przedstawić w postaci iloczynu dwóch wielomianów niższych stopni.

Tabela 1: Parametry algorytmu AES [2]

Długość klucza(w słowach/bajtach/bitach)	4/16/128	6/24/192	8/32/256
Rozmiar bloku wejściowego (w słowach/bajtach/bitach)	4/16/128	4/16/128	4/16/128
Liczba rund	10	12	14
Długość podklucza rundy (w słowach/bajtach/bitach)	4/16/128	4/16/128	4/16/128
Rozmiar rozwiniętego podklucza (w słowach/bajtach)	44/176	52/208	60/240

2 Ciasto z jabłkami i żurawiną

Ciasto z jabłkami i żurawiną [3] to fantastyczna szarlotka dla fanów żurawiny. Połączenie jabłek i świeżej żurawiny jest bezbłędne. Ciasta nie trzeba chłodzić i wstępnie podpiekać, dlatego przygotowanie nie powinno nam zająć dużo czasu. Świeża żurawina jest obecnie w sezonie więc korzystajmy z tego dobrodziejstwa, choć w przepisie bez problemu i żadnych dodatkowych zmian można użyć żurawiny mrożonej. Polecam!

Składniki na ciasto

- 300 g mąki pszennej
- 200 g masła
- 1 łyżeczka proszku do pieczenia
- 1 łyżeczka zmielonego cynamonu
- 1 duże jajko
- 1 żółtko, z dużego jajka
- 110 g jasnego miałkiego brązowego cukru

Wszystkie składniki na ciasto umieścić w misie malaksera i zmiksować do połączenia. Otrzymane ciasto będzie bardzo gęste, wręcz „ciasteczkowo" gęste. Jeśli ciasto będzie mocno klejące można je schłodzić w lodówce przez około 60 minut.

Kwadratową formę o boku 24 cm wyłożyć papierem do pieczenia, sam spód. Ciasto podzielić na 2 równe części. Pierwszą częścią ciasta wylepić spód formy, na nie równomiernie wyłożyć nadzienie jabłkowo – żurawinowe, a na górę wyłożyć drugą część ciasta – w kawałeczkach.

Ciasto z jabłkami i żurawiną piec w temperaturze 180ºC, najlepiej bez termoobiegu (czyli z grzaniem góra-dół), przez około 50 minut. Po wystudzeniu można oprószyć dodatkowym cukrem pudrem.

Składniki na nadzienie jabłkowo - żurawinowe

- 600 g jabłek odmiany szarlotkowej
- 300 g żurawiny
- 1/4 szklanki cukru (lub mniej, do smaku)
- 1 łyżeczka zmielonego cynamonu
- 1 łyżka soku z cytryny
- 1 łyżka skrobi ziemniaczanej

Jabłka umyć, obrać, usunąć gniazda nasienne a następnie pokroić w półplasterki.

Pokrojone jabłka umieścić w garnku, dodać żurawinę, cukier, cynamon i sok z cytryny, następnie wymieszać. Pogotować przez kilka minut do wstępnego odparowania wody i popękana żurawiny. Następnie oprószyć przez sitko skrobią ziemniaczaną i wymieszać. Zdjąć z palnika, nie trzeba studzić (można gorące wyłożyć na przygotowane ciasto w formie).

Literatura

[1] William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych* Helion, 2012, str. 198-200

[2] William Stallings, *Kryptografia i bezpieczeństwo sieci komputerowych* Helion, 2012, str. 204

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