04. Počítání s polynomy, jednoduchá implementace AES-128

Počítání s polynomy (seminář)

1. Základní operace s polynomy nad GF(2)

Polynom = mnohočlen. Budeme se zabývat polynomy s binárními koeficienty, tedy $a(x) \in GF(2)[x], a(x) = \sum_{i=0}^{n} a_i x^i = \{a_n a_{n-1} \dots a_1 a_0\}$

- Zobrazení polynomů do bitů (bajtů, slov)
- Sčítání, odčítání – v koeficientech modulo 2, tedy XOR
- Násobení – jako na základní škole, ale všechno mod 2, nejsou přenosy
- Dělení $a(x) : b(x) = q(x)$, zbytek $r(x)$. Stupeň polynomu $a(x)$ je $deg\ a(x)$
  - $a(x)$ – dělenec
  - $b(x)$ – dělitel
  - $q(x)$ – podíl
  - $r(x)$ – zbytek
  - Je-li $deg\ a(x) \geq deg\ b(x)$, bude podíl nenulový, musíme dělit
  - Jinak $deg\ a(x) < deg\ b(x)$, a pak $q(x) = 0$ a $r(x) = a(x)$

Násobení průchodem násobitele od LSB

```
   1010
  *0101
   ----
   1010
  0000
 1010
0000
-------
0100010
```

Násobení průchodem násobitele od MSB

```
 1010
*0101
 ----
 1010
  0000
```

```
  1010
   0000
-------
0100010
```

2. Operace s polynomy modulo polynom

$a(x) \in GF(2)[x]/m(x)$, kde $m(x)$ je nerozložitelný polynom nad $GF(2)$.

Ex: $m(x) = x^4 + x + 1 = \{10011_2\}$

- Sčítání, odčítání – viz výše
- Redukce modulo – pomocí dělení, výpočet zbytku
- Násobení modulo – odděleně vs prokládaně

Násobení od MSB

```
s = 0
for i = n-1 downto 0
  s = s * x        (shift)
  s = s mod m      (reduction modulo)
  s = s + a * b_i  (add)
```

Shift + redukce = funkce `xtime()` v AES

Násobení od LSB

```
s = 0
for i = 0 to n-1
  s = s + a * b_i  (add)
  a = a * x        (shift operand a)
  a = a mod m      (reduction modulo)
```

3. Operace v AES

Standard šifry AES: [FIPS PUB 197 (https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf)](https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf) .

- Notace AES polynomů
- Základní operace, funkce `xtime()`

Šifrování

- SubBytes
- ShiftRows
- MixColumns
- AddRoundKey
- Key expansion

Dešifrování

- InvSubBytes
- InvShiftRows
- InvMixColumns
- AddRoundKey
- Key expansion

Jednoduchá implementace AES-128

Dokončete jednoduchou a přímočarou implementaci šifry AES-128. Jedná se pouze o blokovou transformaci šifrování, bez zarovnání.

Šablona a testovací kód: aestest4_tmpl.cpp (../files/aestest4_tmpl.cpp)

- Použitelné pod Windows nebo Linux, C++ nebo C
- Doplňte chybějící datové struktury (SBOX) a kód.
- Jednoduchá implementace, neoptimální rychlost ani odolnost proti útokům
- Vnitřní stav se skládá z 4 * 32bitových slov
    - Každé slovo obsahuje 1 sloupec stavové matice
    - V nejnižším bajtu slova je uložen bajt z 0. řádku, v nejvyšším je bajt z 3. řádku, tedy LSB first.
- Some basic functional testing is included
- Specification: FIPS-197 (https://csrc.nist.gov/csrc/media/publications/fips/197/final/documents/fips-197.pdf)

Tipy a poznámky

Odlišnosti od pseudokódu v standardu

- Pole `state` je pole 4 32bitových (čtyřbajtových) slov, po sloupcích, bajt číslo 0 je uložen na nejnižší pozici slova 0, bajt č. 15 je uložen na nejvyšší pozici slova 3

Expanze klíče

Expanze klíče je zjednodušená oproti specifikaci, protože máme jen 128 bitů klíče, což znamená 4 slova.

Funkce `expandKey` předpokládá, že délka klíče je dána napevno.

(Nk=4, Nr=10, Nb je vzdy 4). Standard o těchto parametrech uvádí:

- Nb = Number of columns (32-bit words) comprising the State. For this standard, Nb = 4. (Also see Sec. 6.3.)
- Nk = Number of 32-bit words comprising the Cipher Key. For this standard, Nk = 4, 6, or 8. (Also see Sec. 6.3.)
- Nr = Number of rounds, which is a function of Nk and Nb (which is fixed). For this standard, Nr = 10, 12, or 14. (Also see Sec. 6.3.)

Testovací data

Navíc k testovacím vektorům v standardu máte k dispozici další výpis z průběhu šifrování.

- IN is the input data block byte by byte (= also word by word, LSB first)
- K00 is the input key, used before the first round
- K01 to K10 are the expanded round keys
- ARK is after AddRoundKey
- SB is after SubBytes
- SR is after ShiftRows
- MC is after MixColumns
- Out is the output block

```
IN:  ab cd ef 01 23 45 67 89 ab cd ef 01 23 45 67 89
K00: 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
K01: c0 39 34 78 84 6c 52 0f 0c f5 f8 b4 c0 28 16 4b
K02: f6 7e 87 c2 72 12 d5 cd 7e e7 2d 79 be cf 3b 32
K03: 78 9c a4 6c 0a 8e 71 a1 74 69 5c d8 ca a6 67 ea
K04: 54 19 23 18 5e 97 52 b9 2a fe 0e 61 e0 58 69 8b
K05: 2e e0 1e f9 70 77 4c 40 5a 89 42 21 ba d1 2b aa
K06: 30 11 b2 0d 40 66 fe 4d 1a ef bc 6c a0 3e 97 c6
K07: c2 99 06 ed 82 ff f8 a0 98 10 44 cc 38 2e d3 0a
K08: 73 ff 61 ea f1 00 99 4a 69 10 dd 86 51 3e 0e 8c
K09: da 54 05 3b 2b 54 9c 71 42 44 41 f7 13 7a 4f 7b
K10: 36 d0 24 46 1d 84 b8 37 5f c0 f9 c0 4c ba b6 bb
ARK: ab dc cd 32 67 10 01 fe 23 54 45 ba ef 98 89 76
SB:  62 86 bd 23 85 ca 7c bb 26 20 6e f4 df 46 a7 38
SR:  62 ca 6e 38 85 20 a7 23 26 46 bd bb df 86 7c f4
MC:  d7 67 3c 72 f5 14 95 55 80 cd d7 fc bc b8 a6 73
ARK: 17 5e 08 0a 71 78 c7 5a 8c 38 2f 48 7c 90 b0 38
SB:  f0 58 30 67 a3 bc c6 be 64 07 15 52 10 60 e7 07
```

```
SR:  f0 bc 15 07 a3 07 e7 67 64 60 30 be 10 58 c6 52
MC:  36 ab 6f ac d4 f8 d8 d0 e6 4a bd 9b 5c a3 29 0a
ARK: c0 d5 e8 6e a6 ea 0d 1d 98 ad 90 e2 e2 6c 12 38
SB:  ba 03 9b 9f 24 87 d7 a4 46 95 60 98 98 50 c9 07
SR:  ba 87 60 07 24 95 c9 9f 46 50 9b a4 98 03 d7 98
MC:  9a 08 f4 3c ba ca 82 15 43 f4 cc 52 61 64 9d 4c
ARK: e2 94 50 50 b0 44 f3 b4 37 9d 90 8a ab c2 fa a6
SB:  98 22 53 53 e7 1b 0d 8d 9a 5e 60 7e 62 25 2d 24
SR:  98 1b 60 24 e7 5e 2d 53 9a 25 53 8d 62 22 0d 7e
MC:  42 2a 2f 80 49 7f 16 e7 9e a8 95 c2 d1 4f d8 75
ARK: 16 33 0c 98 17 e8 44 5e b4 56 9b a3 31 17 b1 fe
SB:  47 c3 fe 46 f0 9b 1b 58 8d b1 14 0a c7 f0 c8 bb
SR:  47 9b 14 bb f0 b1 c8 46 8d f0 fe 58 c7 c3 1b 0a
MC:  97 ed 22 2b bd 8c 00 fe ac 37 72 32 da 7d 2c 9e
ARK: b9 0d 3c d2 cd fb 4c be f6 be 30 13 60 ac 07 34
SB:  56 d7 eb b5 bd 0f 29 ae 42 ae 04 7d d0 91 c5 18
SR:  56 0f 04 18 bd ae c5 b5 42 91 eb ae d0 d7 29 7d
MC:  a1 5c 79 c1 f8 1b 46 c6 69 f3 f7 fb 8d 63 d2 6f
ARK: 91 4d cb cc b8 7d b8 8b 73 1c 4b 97 2d 5d 45 a9
SB:  81 e3 1f 4b 6c ff 6c 3d 8f 9c b3 88 d8 4c 6e d3
SR:  81 ff b3 d3 6c 9c 6e 4b 8f 4c 1f 3d d8 e3 6c 88
MC:  63 79 6d 69 42 b6 f1 d0 f3 0b ba a3 71 39 60 f7
ARK: a1 e0 6b 84 c0 49 09 70 6b 1b fe 6f 49 17 b3 fd
SB:  32 e1 7f 5f ba 3b 01 51 7f af bb a8 3b f0 6d 54
SR:  32 3b bb 54 ba af 6d 5f 7f f0 7f 51 3b e1 01 a8
MC:  c6 c6 98 7e b7 17 2e a9 db 54 82 ac e7 49 3b e6
ARK: b5 39 f9 94 46 17 b7 e3 b2 44 5f 2a b6 77 35 6a
SB:  d5 12 99 22 5a f0 a9 11 37 1b cf e5 4e f5 96 02
SR:  d5 f0 cf 02 5a 1b 96 22 37 f5 99 11 4e 12 a9 e5
MC:  77 66 a6 5f 2d ef 10 27 e2 67 d8 17 e6 6f 21 b8
ARK: ad 32 a3 64 06 bb 8c 56 a0 23 99 e0 f5 15 6e c3
SB:  95 23 0a 43 6f ea 64 b1 e0 26 ee e1 e6 59 9f 2e
SR:  95 ea ee 2e 6f 26 9f 43 e0 59 0a b1 e6 23 64 e1
ARK: a3 3a ca 68 72 a2 27 74 bf 99 f3 71 aa 99 d2 5a
Out: a3 3a ca 68 72 a2 27 74 bf 99 f3 71 aa 99 d2 5a
```