

WSTĘP DO KRYPTOGRAFII

ĆWICZENIA VI
(powtórzenie przed kolokwium)

Informacja: kolokwium odbędzie się 18 XII 2004, od godziny 10:30 do 12:00 w sali A2. Dozwolone gadżety to czysty papier, długopis oraz kalkulator (niezintegrowany z innym urządzeniem np. telefon, zegarek).

Zagadnienia:

- szyfr Playfaira,
- rekurencja i funkcje tworzące,

- prawdopodobieństwo zupełne, wzór Bayesa,
- transformata Walsh-Hadamarda,
- rejestr LFSR, szyfr Vernama,
- liniowe równania modularne,
- liczby pseudopierwsze Millera-Rabina.

Zadanie 1:

Używając szyfru Playfaira dla poniższej macierzy podstawień:

- zaszyfruj tekst tajny $P = \text{matematyka}$,
- odszyfruj tekst jawny $C = \text{HPGTBJSOWN}$.

| | | | | |
|---------------|------------------------|---------------|---------------|---------------|
| S/ Š | T | O/ Ó | L/ Ł | A/ Ą |
| R | Z/ $\text{Ž}/\text{Ž}$ | B | C/ Č | D |
| E/ Ě | F | G | H | I |
| J | K | M | N/ Ň | P |
| U | W | X | Y | ' _' |

Rozwiązanie:

- tekst tajny $\mathbf{P} = \text{matematyka} = \text{ma te ma ty ka} \mapsto \mathbf{C} = \text{PO SF PO LW PT} = \text{POSFPOLWPT},$
- tekst jawny $\mathbf{C} = \text{HPGTBJSOWN} = \text{HP GT BJ SO WN} \mapsto \mathbf{P} = \text{in fo rm at yk} = \text{informatyk}.$



Zadanie 2:

Dla podanego poniżej ciągu rekurencyjnego G :

- podaj funkcję tworzącą tego ciągu,
- podaj postać zwartą dla n -tego elementu tego ciągu.

$$G = \begin{cases} g_0 = 2 & \text{dla } n = 0 \\ g_1 = 3 & \text{dla } n = 1 \\ k_n = 5 \cdot g_{n-1} + 7 \cdot g_{n-2} & \text{dla } n \geq 2 \end{cases}$$

Rozwiązanie:

- określamy ogólne równanie rekurencyjne elementu g_n wiążące wszystkie wartości naturalne zmiennej indeksującej n , czyli

$$g_n = 5 \cdot g_{n-1} + 7 \cdot g_{n-2} + 2 \cdot [n = 0] - 7 \cdot [n = 1],$$

- mnożymy obie strony równania przez z^n (z - współczynnik pomocniczy) i sumujemy po wszystkich n , czyli

$$\begin{aligned} g_n \cdot z^n &= 5 \cdot g_{n-1} \cdot z^n + 7 \cdot g_{n-2} \cdot z^n + \\ &\quad 2 \cdot [n = 0] \cdot z^n - 7 \cdot [n = 1] \cdot z^n \\ \sum_n g_n \cdot z^n &= 5 \cdot \sum_n g_{n-1} \cdot z^n + 7 \cdot \sum_n g_{n-2} \cdot z^n + \\ &\quad 2 \cdot \sum_n [n = 0] \cdot z^n - 7 \cdot \sum_n [n = 1] \cdot z^n \\ \sum_n g_n \cdot z^n &= 5 \cdot \sum_n g_n \cdot z^{n+1} + 7 \cdot \sum_n g_n \cdot z^{n+2} + 2 - 7 \cdot z \end{aligned}$$

- dla $\sum_n g_n \cdot z^n$ wprowadzamy oznaczenie $G(z)$ i przepisujemy równanie rekurencyjne używając nowego symbolu (otrzymujemy funkcję tworzącą rozważanego ciągu rekurencyjnego):

$$G(z) = 5 \cdot G(z) \cdot z + 7 \cdot G(z) \cdot z^2 + 2 - 7 \cdot z,$$

- rozwiązujemy równanie (szukamy zwartej postaci) względem $G(z)$, czyli

$$G(z) = \frac{2 - 7 \cdot z}{1 - 5 \cdot z - 7 \cdot z^2},$$

- niech ρ_1, ρ_2 będą odwrotnościami rozwiązań równania $1 - 5 \cdot z - 7 \cdot z^2 = 0$, $P(z) = 2 - 7 \cdot z$ oraz $Q(z) = 1 - 5 \cdot z - 7 \cdot z^2$. Jeżeli $\rho_1 \neq \rho_2$ i stopień wielomianu $P(z)$ jest mniejszy od stopnia wielomianu $Q(z)$ to postać zwarta liczby g_n to:

$$g_n = \sum_{i=1}^2 a_i \cdot \rho_i^n, \text{ gdzie } a_i = \frac{-\rho_i \cdot P\left(\frac{1}{\rho_i}\right)}{Q'\left(\frac{1}{\rho_i}\right)}.$$

Zatem:

$$1 - 5 \cdot z - 7 \cdot z^2 = 0 \Rightarrow \rho_1 = \frac{5 + \sqrt{53}}{2} \wedge \rho_2 = \frac{5 - \sqrt{53}}{2},$$

więc

$$\begin{aligned} g_n &= a_1 \cdot \rho_1^n + a_2 \cdot \rho_2^n \\ &= \frac{-\rho_1 \cdot P\left(\frac{1}{\rho_1}\right)}{Q'\left(\frac{1}{\rho_1}\right)} \cdot \rho_1^n + \frac{-\rho_2 \cdot P\left(\frac{1}{\rho_2}\right)}{Q'\left(\frac{1}{\rho_2}\right)} \cdot \rho_2^n, \\ &= \frac{-\rho_1 \cdot \left(2 - 7 \cdot \frac{2}{5 + \sqrt{53}}\right)}{Q'\left(\frac{1}{\rho_1}\right)} \cdot \rho_1^n + \frac{-\rho_2 \cdot \left(2 - 7 \cdot \frac{2}{5 - \sqrt{53}}\right)}{Q'\left(\frac{1}{\rho_2}\right)} \cdot \rho_2^n \end{aligned}$$

gdzie $Q'(z) = -5 - 14 \cdot z$, czyli postać zwarta n -tego elementu ciągu rekurencyjnego to:

$$g_n = \frac{-\rho_1^{n+1} \cdot \left(2 - \frac{14}{5 + \sqrt{53}}\right)}{-5 - \frac{28}{\rho_1}} + \frac{-\rho_2^{n+1} \cdot \left(2 - \frac{14}{5 - \sqrt{53}}\right)}{-5 - \frac{28}{\rho_2}}$$

$$\begin{aligned}
&= \frac{\rho_1^{n+1} \cdot \left(2 - \frac{14 \cdot (5 - \sqrt{53})}{-48}\right)}{5 + \frac{28}{5 + \sqrt{53}}} + \frac{\rho_2^{n+1} \cdot \left(2 - \frac{14 \cdot (5 + \sqrt{53})}{-48}\right)}{5 + \frac{28}{5 - \sqrt{53}}} \\
&= \frac{\rho_1^{n+1} \cdot \left(2 - \frac{7 \cdot (5 - \sqrt{53})}{-24}\right)}{5 + \frac{28 \cdot (5 - \sqrt{53})}{-48}} + \frac{\rho_2^{n+1} \cdot \left(2 - \frac{7 \cdot (5 + \sqrt{53})}{-24}\right)}{5 + \frac{28 \cdot (5 + \sqrt{53})}{-48}} \\
&= \frac{\rho_1^{n+1} \cdot \left(\frac{-13 - 7 \cdot \sqrt{53}}{-24}\right)}{\frac{5 + \sqrt{53}}{2}} + \frac{\rho_2^{n+1} \cdot \left(\frac{-13 + 7 \cdot \sqrt{53}}{-24}\right)}{\frac{5 - \sqrt{53}}{2}}.
\end{aligned}$$



Zadanie 3:

Na pierwszym roku pewnego wydziału są 120 słuchaczy, pochodzących z trzech grup społecznych: z miast, z miasteczek oraz ze wsi. Liczebność słuchaczy z odpowiednich grup to kolejno: 50, 40 i 30 osób. Wiadomo, że prawdopodobieństwa ukończenia studiów w terminie dla słuchaczy rozważanych grup społecznych wynoszą odpowiednio: 0,3, 0,4 i 0,5. Wybieramy losowo jednego słuchacza z pierwszego roku studiów, oblicz:

- prawdopodobieństwo \mathcal{P}_1 tego, że pochodzi on z miasta,
- prawdopodobieństwo \mathcal{P}_2 tego, że ukończy on terminowo studia,
- prawdopodobieństwo \mathcal{P}_3 tego, że pochodzi on z miasta, jeżeli wiemy, że ukończy terminowo studia.

Rozwiązanie: niech A_1 , A_2 i A_3 oznaczają odpowiednio zdarzenia polegające na tym, że wylosowany student pochodzi z miasta, z miasteczka albo ze wsi. Dalej przez B rozumiemy fakt, że student ukończy terminowo studia. Zatem:

- $\mathcal{P}(A_1) = \frac{5}{12}$, $\mathcal{P}(A_2) = \frac{4}{12}$, $\mathcal{P}(A_3) = \frac{3}{12}$,
- $\mathcal{P}(B|A_1) = \frac{3}{10}$, $\mathcal{P}(B|A_2) = \frac{4}{10}$, $\mathcal{P}(B|A_3) = \frac{5}{10}$,

stąd:

- $\mathcal{P}_1 = \mathcal{P}(A_1) = \frac{5}{12} \approx 0,42$,

- $\mathcal{P}_2 = \mathcal{P}(B) = \sum_{i=1}^3 \mathcal{P}(A_i) \cdot \mathcal{P}(B|A_i) = \frac{5 \cdot 3 + 4 \cdot 4 + 3 \cdot 5}{12 \cdot 10} = \frac{46}{120} \approx 0,38,$

- $\mathcal{P}_3 = \mathcal{P}(A_1|B) = \frac{\mathcal{P}(A_1) \cdot \mathcal{P}(B|A_1)}{\mathcal{P}(B)} = \frac{\frac{5}{12} \cdot \frac{3}{10}}{\frac{46}{120}} = \frac{15}{46} \approx 0,35.$



Zadanie 4:

Niech $f : Z_2^3 \rightarrow Z_2$ będzie funkcją boolowską zgodną z tablicą prawdy

$$X = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Podaj szósty element tablicy prawdy funkcji $F : Z_2^n \rightarrow \mathbb{R}$ (tj. $F(5)$) będącej transformatą Walsha-Hadamarda funkcji f .

Rozwiązanie: z tablicy prawdy funkcji f odczytujemy, że

$$\begin{aligned}f(0 = 000) &= 1, & f(1 = 001) &= 0, \\f(2 = 010) &= 1, & f(3 = 011) &= 0, \\f(4 = 100) &= 1, & f(5 = 101) &= 1, \\f(6 = 110) &= 1, & f(7 = 111) &= 1.\end{aligned}$$

Zatem:

$$\begin{aligned}F(5 = 101) &= \sum_{i=0}^7 f(i_B) \cdot (-1)^{\langle i_B, 5_B \rangle} \\&= f(000) \cdot (-1)^{\langle 000, 101 \rangle} + f(001) \cdot (-1)^{\langle 001, 101 \rangle} + \\&\quad f(010) \cdot (-1)^{\langle 010, 101 \rangle} + f(011) \cdot (-1)^{\langle 011, 101 \rangle} + \\&\quad f(100) \cdot (-1)^{\langle 100, 101 \rangle} + f(101) \cdot (-1)^{\langle 101, 101 \rangle} + \\&\quad f(110) \cdot (-1)^{\langle 110, 101 \rangle} + f(111) \cdot (-1)^{\langle 111, 101 \rangle} \\&= 1 \cdot (-1)^0 + 0 \cdot (-1)^1 + 1 \cdot (-1)^0 + 0 \cdot (-1)^1 + \\&\quad 1 \cdot (-1)^1 + 1 \cdot (-1)^0 + 1 \cdot (-1)^1 + 1 \cdot (-1)^0 \\&= 1 + 0 + 1 + 0 +\end{aligned}$$

$$= -1 + 1 - 1 + 1$$
$$= 2.$$



Zadanie 5:

Zaszyfruj używając szyfru Vernama napis “KRYPTO” zapisany binarnie względem ośmiobitowych wartości znaków w standardzie ASCII przy założeniu, że generator klucza szyfru jest 5-bitowym układem LFSR inicjowanym wartością 13 z parametrem $m = 3$ (l_4 , l_2 i l_0 są sprzężone). Pamiętaj, że:

$$\text{ASCII}(K) = 75,$$

$$\text{ASCII}(R) = 82,$$

$$\text{ASCII}(Y) = 89,$$

$$\text{ASCII}(P) = 80,$$

$$\text{ASCII}(T) = 84,$$

$$\text{ASCII}(O) = 79.$$

liczba dziesiętna 13 odpowiada pięciobitowemu ciągowi binarnemu postaci 01101, czyli klucz rejestru LFSR to $K = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \end{bmatrix}$.

| czas | l_4 | l_3 | l_2 | l_1 | l_0 | sprzężenie | out |
|------|-------|-------|-------|-------|-------|------------|-----|
| 0 | 0 | 1 | 1 | 0 | 1 | - | - |
| 1 | 0 | 0 | 1 | 1 | 0 | 0 | 1 |
| 2 | 1 | 0 | 0 | 1 | 1 | 1 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 | 0 | 1 |
| 4 | 1 | 0 | 1 | 0 | 0 | 1 | 1 |
| 5 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |
| 6 | 0 | 0 | 1 | 0 | 1 | 0 | 0 |
| 7 | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| 8 | 0 | 0 | 0 | 0 | 1 | 0 | 0 |
| 9 | 1 | 0 | 0 | 0 | 0 | 1 | 1 |
| 10 | 1 | 1 | 0 | 0 | 0 | 1 | 0 |
| 11 | 1 | 1 | 1 | 0 | 0 | 1 | 0 |
| 12 | 0 | 1 | 1 | 1 | 0 | 0 | 0 |
| 13 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |

| | | | | | | | |
|----|---|---|---|---|---|---|---|
| 14 | 1 | 1 | 0 | 1 | 1 | 1 | 1 |
| 15 | 0 | 1 | 1 | 0 | 1 | 0 | 1 |

Na podstawie powyższej tabeli odczytujemy cykl układu LFSR:

101100101000011.

Następnie ustalamy binarne (ośmiobitowe) reprezentacji znaków napisu "PJWSTK":

- $\text{ASCII}(K) = 75 = 01001011,$
- $\text{ASCII}(R) = 82 = 01010010,$

- $\text{ASCII}(Y) = 89 = 01011001,$
- $\text{ASCII}(P) = 80 = 01010000,$
- $\text{ASCII}(T) = 84 = 01010100,$
- $\text{ASCII}(O) = 79 = 01001111.$

Zatem ciąg binarny jaki mamy zamiar szyfrować to:

01001011|01010010|01011001|01010000|01010100|01001111.

Generator klucza szyfru jest układem okresowym o okresie rozmiaru 15. Na tej podstawie dokonujemy szyfrowania metodą Vernama:

01001011|01010010|01011001|01010000|01010100|01001111 \oplus
10110010|10000111|01100101|00001110|11001010|00011101 =
11111001|11010101|00111101|01011110|10011110|01010010.

Teraz ciąg wynikowy

11111001|11010101|00111101|01011110|10011110|01010010

przekształcamy do postaci znaków w standardzie ASCII, otrzymujemy:

ASCII(11111001) = ASCII(249),
ASCII(11010101) = ASCII(213),
ASCII(00111101) = ASCII(61),
ASCII(01011110) = ASCII(94),
ASCII(10011110) = ASCII(158),
ASCII(01010010) = ASCII(82).



Zadanie 6:

Rozwiąż równanie

$$17 \cdot z \equiv 19 \pmod{100}.$$

Rozwiązanie: przyjmujemy, że $a = 17$, $b = 19$ oraz $k = 100$. Obliczamy używając rozszerzony algorytm Euklidesa $NWD(17, 100) = n = x \cdot 17 + y \cdot 100$:

| a | b | $\lfloor a/b \rfloor$ | n | x | y |
|-----|-----|-----------------------|-----|-----|-----|
| 17 | 100 | - | - | - | - |
| 100 | 17 | - | - | - | - |
| 17 | 15 | - | - | - | - |
| 15 | 2 | - | - | - | - |
| 2 | 1 | - | - | - | - |
| 1 | 0 | - | 1 | 1 | 0 |
| 2 | 1 | 2 | 1 | 0 | 1 |
| 15 | 2 | 7 | 1 | 1 | -7 |
| 17 | 15 | 1 | 1 | -7 | 8 |
| 100 | 17 | 5 | 1 | 8 | -47 |
| 17 | 100 | 0 | 1 | -47 | 8 |

Ponieważ $19 \bmod 1 = 0$ to

$$z = (-47) \cdot 19/1 \bmod 100 = 7.$$

Zatem procedura wypisze jedno rozwiązanie:

- $z_0 = (z + 0 \cdot 100/1) \bmod 100 = (7 + 0) \bmod 100 = 7.$



Zadanie 7:

Stwierdź, czy liczba 133 jest liczbą pseudopierwszą Millera-Rabina przy podstawie 3.

Rozwiązanie: nasze zadanie sprowadza się do obliczenia wartości wyrażenia $3^{132} \bmod 133$. Liczba 132 zapisana w postaci binarnej to ciąg bitów

10000100.

Dalej wykonujemy obliczenia:

| b_i | tmp1a | tmp2a | tmp1b | tmp2b |
|-------|-------|-------|-------|-------|
| - | 0 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 | 3 |
| 0 | 2 | 9 | 2 | 9 |
| 0 | 4 | 81 | 4 | 81 |
| 0 | 8 | 44 | 8 | 44 |
| 0 | 16 | 74 | 16 | 74 |
| 1 | 32 | 23 | 33 | 69 |
| 0 | 66 | 106 | 66 | 106 |
| 0 | 132 | 64 | 132 | 64 |

Liczba 133 nie jest więc liczbą pseudopierwszą Millera-Rabina przy podstawie 3, nie jest także liczbą pseudopierwszą Fermata (przy tej samej podstawie). Liczba ta jest zatem liczbą złożoną ($133 = 7 \cdot 19$).

