Spočtěte $|\log_7 11|_{13}$ v multiplikativní grupě. v aditivní... 3

5 $7^x = 11 \mod 13 = 5$ $7 \cdot x = 11 \mod 13$

Vypočítejte hodnotu Eulerovy funkce čísla 3575. 3

EulerPhi[3575]

- ✔ − ✖ 480
- ✔ − ✖ 2400
- ✔ − ✖ 2860
- ✔ − ✖ 3574

Afinní šifra šifruje s koeficienty $a = 73$ a $b = 85$ v modulu $m = 256$. Vyberte správné šifrovací a dešifrovací předpisy: 3

- ✔ − ✖ $c = |85 \cdot p + 73|_{256}$
- ✔ − ✖ $p = |73^{-1} \cdot c + 85|_{255}$
- ✔ − ✖ $p = |249 \cdot c + 83|_{256}$
- ✔ − ✖ $c = |73 \cdot p + 85|_{256}$

$c = |ap + b|_m = |73p + 85|_{256}$

$p = |a^{-1} \cdot (c - b)|_m$

$= |249 \cdot (c - 85)|_m$

- $|-85 \cdot 73^{-1}|_{256} = 83$ ✖

Je dán klíč - šifrovací matice $\mathbb{A}$ pro Hillovu šifru. Spočítejte dešifrovací matici, když víte, že byla použita anglická abeceda o 26 znacích.

$$\mathbb{A} = \begin{pmatrix} 3 & 7 \\ 5 & 2 \end{pmatrix}$$

Výslednou matici zapište jako serializaci matice po řádcích. Tedy matice $\mathbb{A}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ bude vypadat jako "a,b,c,d" (bez uvozovek, oddělené čárkou, kladná čísla). 3

8,11,19,25 A^{-1} = Inverse[{{3, 7}, {5, 2}}, Modulus → 26]

Frekvenční analýzou jsme zjistili, že nejčetnější písmeno v šifrovém textu s abecedou o délce 26 znaků je písmeno B. Druhé nejčetnější je písmeno K. Víme, že otevřený text je psán anglicky. Jakým šifrovacím předpisem byl (pravděpodobně afinní šifrou) šifrován ST = IBAAH? Určete koeficienty a a b. Déle dešifrujte ST, za předpokladu, že četnost znaků zprávy odpovídá průměrné četnosti znaků v jazyku. Odpověď uveďte ve formátu "a,b,OT" (bez uvozovek, oddělené čárkou).

3

E → B T → K A = 11 ; B = 9 Hello

H → I, L → A, O → H

$c = |11p + 9|_{26}$

$2 = |4A + B|_{26}$

$10 = |19A + B|_{26}$

$|20A + 5B|_{26} = |19A + B|_{26}$

$|220 + 45|_{26} = 265$

$|209 + 9|_{26} = 218$

11,9,HELLO

Je dán šifrový text ST = GWGTENYR, který je zašifrovaný Hillovou šifrou nad abecedou s 26 znaky maticí

$A^{-1} = \text{Inverse}[\{\{3,2\},\{7,5\}\}, \text{Modulus} \to 26]$

$$A = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix}$$

Určete otevřený text OT.

$$A^{-1} = \begin{pmatrix} 5 & 24 \\ 19 & 3 \end{pmatrix}$$

3

MYSPULIN

A	0	N	13
B	1	O	14
C	2	P	15
D	3	Q	16
E	4	R	17
F	5	S	18
G	6	T	19
H	7	U	20
I	8	V	21
J	9	W	22
K	10	X	23
L	11	Y	24
M	12	Z	25

$$\left(\begin{array}{cc|cc} 3 & 2 & 1 & 0 \\ 7 & 5 & 0 & 1 \end{array}\right)_{26} \left(\begin{array}{cc|cc} 1 & 0 & 5 & 24 \\ 7 & 5 & 0 & 1 \end{array}\right)_{26} \sim \left(\begin{array}{cc|cc} 1 & 0 & 5 & 24 \\ 0 & 5 & -35 & -11 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 5 & 24 \\ 0 & 1 & 19 & 3 \end{array}\right)$$

$: 17 \quad : 15$

$5 \cdot 21 = 105 \ \%\ 26 = 1 \qquad 17 \cdot 21 \ \%\ 26 = 19 \qquad 15 \cdot 21 \ \%\ 26 = 3$

Spočítejte

$$\left| \frac{208^{192} + 29^{992}}{3^{21}} \right|_{22}$$

$12 \quad 5 \quad 15$

Výsledek uveďte ve formě mezivýpočtů, tj. : $|208^{192}|_{22}$, $|29^{992}|_{22}$, $\left|(3^{21})^{-1}\right|_{22}$ a celkový výsledek. Ukázková odpověď tedy může vypadat (bez uvozovek) takto: "1,1,1,1"

3

12,5,15,13 $= \frac{17}{3} = 17 \cdot 3^{-1}$

Určete takovou dvojici celých čísel a a b tak, aby platila rovnost $\gcd(2013, 823) = 2013 \cdot a + 823 \cdot b$ a zároveň aby byl koeficient b multiplikativní inverze čísla 823 v modulu 2013. Čísla zapište v tomto pořadí, oddělená čárkou a mezerou.

3

-74, 181

```
In[47]:= Inverse[{{823}}, Modulus → 2013]
Out[47]= {{181}}

In[48]:= GCD[2013, 823]
Out[48]= 1

In[50]:= NSolve[148 963 + 2013 tmp == 1, {tmp}, ℝ]
Out[50]= {{tmp → -74.}}
```

Anička, Bob a Cyril spolu chtějí komunikovat a za pomocí Diffie-Hellmanova algoritmu si chtějí vyměnit tajný klíč K. Společně si zvolili parametry $a = 5$ a $m = 23$. Anička má subklíč $k_A = 5$, Bob $k_B = 2$ a Cyril $k_C = 3$. Jaký bude jejich sdílený klíč K?

3

16

$k_A = 5$, $k_B = 2$, $k_C = 3$ | $a = 5$, $m = 23$, $K = ?$ (generátor násobící grupy mod m, velké prvočíslo $\wedge$ $\gcd(m, a) = 1$)

- $\gcd(k_i, m-1) = 1$
- $y_i = |a^{k_i}|_m$

$y_A = |a^{k_A}|_m = 20$, $y_B = |a^{k_B}|_m = 2$, $y_C = |a^{k_C}|_m = 10$

$y_{AB} = |y_B^{k_A}|_{23} = |2^5|_{23} = 9$, $y_{BC} = |y_C^{k_B}|_{23} = |10^2|_{23} = 8$, $y_{CA} = |y_A^{k_C}|_{23} = |20^3|_{23} = 19$

$y_{ABC} = |y_{BC}^{k_A}|_{23} = |8^5|_{23} = 16$, $y_{BCA} = |y_{CA}^{k_B}|_{23} = |19^2|_{23} = 16$, $y_{CAB} = |y_{AB}^{k_C}|_{23} = |9^3|_{23} = 16$

Jů a Hele spolu chtějí komunikovat pomocí exponenciální šifry. Zvolí si modul $m = 23$. Která z následujících tvrzení jsou platná?

3

✔ − ✖ Pro exponent $e = 7$ a $ST = 2$ je $OT = 5$.

Exp. š.: $c = |p^e|_m$

✔ − ✖ Exponent $e = 2$ nemůže být použit jako šifrovací klíč.

$2 = |5^7|_{23}$

✔ − ✖ Pro $e = 2$ je dešifrovací klíč $d = 13$.

$C = |{}^{-3}|_{23}$

✔ − ✖ Pro exponent $e = 2$ a $ST = 3$ je $OT = 17$.

✔ − ✖ Pro $e = 7$ je dešifrovací klíč $d = 19$.

- Musí platit: $p = |c^d|_m = |p^{ed}|_m$

$d \equiv e^{-1} \pmod{m-1}$

$\gcd(e, m-1) = 1$

```
In[32]:= Inverse[{{7}}, Modulus → 23 - 1]
Out[32]= {{19}}
```

Máme šifru založenou na afinní transformaci $c = |ap + b|_{26}$. Které parametry a a b je možné použít?

- ✔ − ✖ $a = 1, b = 10$
- ✔ − ✖ $a \in \{\forall x \in \mathbb{Z}_{26} | gcd(x, 26) = 1\}, b \in \mathbb{Z}$
- ✔ − ✖ $a = 3, b = 20$
- ✔ − ✖ $a = 6, b = 23$

Výborně! Otázka byla odpovězena správně.

další otáz

Jediný požadavek je zde na nesoudělnost **a** s modulem (**gcd(a,26) == 1**)

Mějme abecedu o 45 znacích. Kolik existuje různých klíčů pro afinní šifru? (Různých znamená, že definují různé šifrovací předpisy.)

3

- ✔ − ✖ $\varphi(45) \cdot \varphi(45)$
- ✔ − ✖ 2025
- ✔ − ✖ $\varphi(45) \cdot 45$
- ✔ − ✖ $24 \cdot 24$

Určete kanonický rozklad čísla 72900. Odpověď zadávejte jako nenulové exponenty u mocnin jednotlivých prvočítel ve vzestupném pořadí a oddělené čárkou. Obecně pro $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots$ napíšeme "$\alpha_1, \alpha_2, \dots$". Například odpověď pro číslo 14 zapíšeme jako "1,1" (bez uvozovek).

3

2,6,2

In[27]:= `FactorInteger[72900]`

Out[27]= `{{2, 2}, {3, 6}, {5, 2}}`

$= 2^2 \cdot 3^6 \cdot 5^2$

LEAKS

O substitučních šifrách platí následující:

1

- ✔ − ✖ Rozprostírají informaci po délce šifrového textu
- ✔ − ✖ Nemění (nepřeskupují) statistické rozložení četnosti písmen v textu
- ✔ − ✖ Do šifrového textu vnášejí konfúzi
- ✔ − ✖ Zaměňují znaky v textu jinými v abecedě

Dostali jsme za úkol provést kryptoanalýzu afinní šifry. Z frekvenční analýzy víme, že nejčastější znaky ST jsou V(1.) a Q(2.). Předpokládáme, že OT je napsán v angličtině, kde nejčetnější jsou E(1.) a T(2.). Zjistěte klíč pro odhad, kdy zkusíme spárovat znaky z ST na OT přesně podle pořadí jejich četností.

0

- ✔ − ✖ $a = 5, b = 5$
- ✔ − ✖ $a = 21, b = 5$
- ✔ − ✖ $a = 5, b = 17$
- ✔ − ✖ $a = 17, b = 5$

$C = a \cdot T + b \pmod m$

$C = a \cdot T + b \pmod{26}$

$21 = V = |a \cdot \overset{4}{E} + b|_{26}$

$16 = Q = |a \cdot \overset{19}{T} + b|_{26}$

a = 0 n = 13
b = 1 o = 14
c = 2 p = 15
d = 3 q = 16
e = 4 r = 17
f = 5 s = 18
g = 6 t = 19
h = 7 u = 20
i = 8 v = 21
j = 9 w = 22
k = 10 x = 23
l = 11 y = 24
m = 12 z = 25

Kapela **ABBA** chystá nové album, a komunikuje se studiem přes telegramy, které však zašifruje pomocí Hillovy šifry s modulem 26 a velikostí bloku 2. Odchytili jsme na síti jejich komunikaci. Víme, že zpráva začíná názvem kapely, a odchycená komunikace (šifrový text) začíná znaky **BUZZ**. Jaká byla použitá matice pro šifrování? Zapište kladné hodnoty matice po řádcích a oddělené čárkou, např. pro matici

OT = ABBA AB → BU $\begin{pmatrix} 1 & -7 \\ 2 & 15 \end{pmatrix}$
ST = BUZZ BA → ZZ

do odpovědi napište `1,19,2,15`

- Abychom získali $\mathbf{A}$, musíme invertovat matici, se kterou je vynásobena:

$$\left(\begin{smallmatrix} 19 & 7 & 1 & 0 \\ 7 & 4 & 0 & 1 \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 1 & 25 & 11 & 0 \\ 0 & 11 & 1 & 1 \end{smallmatrix}\right) \sim \left(\begin{smallmatrix} 1 & 0 & 4 & 19 \\ 0 & 1 & 19 & 19 \end{smallmatrix}\right).$$ Proto

$$\mathbf{A} = \left|\left(\begin{smallmatrix} 10 & 21 \\ 23 & 25 \end{smallmatrix}\right)\left(\begin{smallmatrix} 4 & 19 \\ 19 & 19 \end{smallmatrix}\right)\right|_{26} = \left(\begin{smallmatrix} 23 & 17 \\ 21 & 2 \end{smallmatrix}\right).$$

0

25,1,25,20

$c_1 = |a_{11} \cdot p_1 + a_{12} \cdot p_2|_m$
$c_2 = |a_{21} \cdot p_1 + a_{22} \cdot p_2|_m$
neboli: $\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \left|\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}\right|_m$
neboli: $c = |Ap|_m$

$$\left|A\begin{pmatrix} A & B \\ B & A \end{pmatrix}\right|_{26} = \left|\begin{pmatrix} B & Z \\ U & Z \end{pmatrix}\right|_{26} \Rightarrow \left|A\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right|_{26} = \left|\begin{pmatrix} 1 & 25 \\ 20 & 25 \end{pmatrix}\right|_{26}$$

$$A = \left|\begin{pmatrix} 1 & 25 \\ 20 & 25 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right|_{26} = \begin{pmatrix} 25 & 1 \\ 25 & 20 \end{pmatrix}$$

$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 20 \end{pmatrix}$
$\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 25 \\ 25 \end{pmatrix}$

Mějme exponenciální šifru, kde $m = 23$ a $e = -3$. (Zde nám nevadí, že je exponent záporný.) Určete d.

3

7

$d \equiv e^{-1} \pmod{m-1} \equiv -3^{-1} \pmod{22} \equiv 7$

Alfons a Berna si chtějí domluvit tajný klíč pomocí Diffie-Hellmanova algoritmu. Společně si zvolili parametry $a = 2$ a $m = 13$. Alfons má subklíč $k_A = 7$ a Berna má $k_B = 5$. Napište hodnoty v pořadí: Co pošle Alfons (y_A), co pošle Berna (y_B), a pak sdílený klíč (K). Odpovědí budou 3 čísla oddělená čárkami. Příklad odpovědi: 2,3,6

3

11,6,7

- $y_A = |2^7|_{13} = 11$
- $y_B = |2^5|_{13} = 6$
- $K = |11^5|_{13} = |6^7|_{13} = 7$

Posíláme Alici naše oblíbené číslo zašifrované algoritmem El Gamal. Alicí zvolené veřejné parametry jsou $(m = 919, g = 431, y_A = 67)$. Námi zvolený parametr $k_B = 69, oblibeneCislo = 42$. Výsledek zapište jako uspořádanou dvojici "(y_B, c)" bez uvozovek, tedy například $(15, 22)$.

3

(486, 767)

$m = 919$ $g = 431$ $y_A = 67$ $k_B = 69$ $p = 42$ $y_B = ?$ $c = ?$

$c = |p \cdot K|_m = |42 \cdot 434|_{919} = 767$

$K = |y_A^{k_B}|_m = |67^{69}|_{919} = 434$

$y_A = |g^{k_A}|_m \Rightarrow k_A = 42$

$y_B = |g^{k_B}|_m = |431^{69}|_{919} = 486$

Označme h jako hashovací funkci SHA-512. Chceme k dané zprávě x_1 nalézt zprávu x_2 různou od x_1 tak, že $h(x_1) = h(x_2)$. Rozhodněte o platnosti následujících tvrzení:

3

- ✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{128}.
- ✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{256}.
- ✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{512}.
- ✔ – ✖ Jedná se o kolizi druhého řádu.

Máme dáno $H(X) = 4$. Tato entropie je maximální možná. Kolik různých zpráv produkuje zdroj X? Jaká je pravděpodobnost každé z nich? Odpověď zadejte jako dvě čísla oddělená čárkou.

3

16, 1/16

Zdroj zpráv X posílá 4 různé zprávy s pravděpodobnostmi $p_1 = \frac{1}{8}, p_2 = \frac{1}{4}, p_3 = \frac{1}{2}$ a $p_4 = \frac{1}{8}$. Jaká je hodnota entropie $H(X)$? Jaká by byla entropie, pokud bychom změnili pravděpodobnosti tak, aby byly všechny stejné? Odpověď zadejte jako dvě čísla oddělená čárkou.

0

1.75, 16

X (2) → $-p_i \cdot \log_2(p_i) \cdot 4$ … $p_i = \frac{1}{4}$

$$H(X) = -\sum_{i=1}^{n} p_i \cdot \log_2(p_i)$$

Máme šifru 3DES-168 a zprávy psané v angličtině ($r = 1.5$). Klíče šifry jsou vybírány náhodně a jsou stejně pravděpodobné. Na základě těch znalostí rozhodněte o platnosti následujících tvrzení:

3

- ✔ − ✖ Při použitém kódování UTF-32 je vzdálenost jednoznačnosti zhruba 5.51 bitů.
- ✔ − ✖ Při použitém kódování ASCII-8bit je vzdálenost jednoznačnosti zhruba 25.85 bajtů.
- ✔ − ✖ Při použitém kódování ASCII-8bit je vzdálenost jednoznačnosti zhruba 25.85 bitů.
- ✔ − ✖ Při použitém kódování UTF-32 je vzdálenost jednoznačnosti zhruba 5.51 bajtů.

- $H(K) = 168$ (entropie klíče)
- $r = 1,5$ $\quad D = 8 - 1,5 = 6,5$ $\quad D = 16 - 1,5 = 14,5$
- ASCII-8: $\delta_U = \frac{H(K)}{D} = \frac{168}{6,5} \doteq 25,85$
- UTF-16: $\delta_U = \frac{H(K)}{D} = \frac{168}{14,5} \doteq 11,59$

- UTF-32: $\frac{168}{30,5} \doteq 5,51$

Máme zdroj zpráv, který generuje nenulové množství zpráv a má minimální možnou entropii. Kolik různých zpráv s nenulovou pravděpodobností generuje? Jaká je jejich pravděpodobnost? Odpověď uveďte jako dvě čísla oddělená čárkou.

3

1,1

protože minimální entropie bude mít 1 bit ... 1 znak
... když je možné vygenerovat max. 1 znak, $P(E) = 1$

Spočítejte entropii $H(X)$, víte-li, že zdroj zpráv X generuje 7 zpráv. Tři z nich mají pravděpodobnost $\frac{1}{4}$ a zbylé čtyři pravděpodobnost $\frac{1}{16}$. Odpověď uveďte jako desetinné číslo, nebo zlomek v základním tvaru.

3

5/2

$$H(X) = -\sum_{i=n}^{n} p_i \cdot \log_2(p_i) = 3\left(-\tfrac{1}{4} \cdot \log_2\left(\tfrac{1}{4}\right)\right) + 4\left(-\tfrac{1}{16} \cdot \log_2\left(\tfrac{1}{16}\right)\right) = 5/2$$

Označme h jako hashovací funkci SHA-512. Chceme nalézt dvě různé zprávy x_1 a x_2 takové, že $h(x_1) = h(x_2)$. Rozhodněte o platnosti následujících tvrzení:

3

- ✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{511}.
- ✔ – ✖ Jedná se o kolizi druhého řádu.
- ✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{512}.
- ✔ – ✖ Jedná se o kolizi prvního řádu.

Bob Vám poslal své oblíbené číslo zašifrované algoritmem El Gamal. Přijatá zpráva je uspořádaná dvojice $(y_B = 316, c = 706)$. Vámi zvolené parametry jsou $(m = 911, g = 421, k_A = 42)$. Dešifrujte přijatou zprávu a zapište výsledek jako desítkové číslo.

3

666

- $y_B = 316$
- $c = 706$

- $m = 911$
- $g = 421$
- $k_A = 42$

- $K = |y_A^{k_B}|_m = |y_B^{k_A}|_m = |316^{42}|_{911} = 540$
- $c = |p \cdot K|_m = 706$
  - $\hookrightarrow p = 666$

- $K = |a^{k_A \cdot k_B}|_m$
- $y_A = |a^{k_A}|_m = |g^{k_A}|_m$

Alenka si vytváří klíče pro RSA. Zvolí si $p = 5$ a $q = 11$. Rozhodněte o pravdivosti následujících tvrzení:

- ✔ – ✖ Jako veřejný exponent lze zvolit $e = 7$.
- ✔ – ✖ Jako veřejný exponent lze zvolit $e = 5$.
- ✔ – ✖ Pokud zvolíme jako veřejný exponent $e = 7$, soukromý exponent je $d = 23$.
- ✔ – ✖ Při volbě veřejného exponentu $e = 7$ dešifruje Alenka zprávu $c = 2$ jako $m = 8$.

Alenka si vytváří klíče pro RSA. Zvolí si $p = 5$ a $q = 11$. Rozhodněte o pravdivosti následujících tvrzení:

3

- ✔ – ✖ Dvojici (n, d) zveřejníme jako soukromý klíč.
- ✔ – ✖ Eulerova funkce modulu je $\varphi(n) = 40$.
- ✔ – ✖ Jako veřejný exponent lze zvolit $e = 7$.
- ✔ – ✖ Pokud zvolíme jako veřejný exponent $e = 7$, soukromý exponent je $d = 23$.

- $n = p \cdot q = 5 \cdot 11 = 55$
- musí platit: $\gcd(e, \phi(n)) = 1$
- $\phi(55) = 40$ ... $\gcd(5, 40) = 5$ ... $\gcd(7, 40) = 1$

- $c = |m^e|_n = |8^7|_{55} = 2$
- $d = |e^{-1}|_{\phi(n)} = |7^{-1}|_{40} = 23$

Jaká je požadovaná délka klíče šifry, aby pro zprávy psané v angličtině ($r = 1.5$) v kódování ASCII-8bit byla vzdálenost jednoznačnosti cca 20 znaků? Předpokládejte, že klíče šifry jsou vybírány náhodně a jsou stejně pravděpodobné.

3

130

$\frac{X}{6,5} = 20$

LEAKS

Jaký je minimální počet testů (každý test s různou bází), které musíme udělat pomocí Rabin-Millerova testu, abychom měli 98.354% jistotu, že zkoumané číslo je prvočíslo? Výsledek zaokrouhlete na celá čísla nahoru. Tedy například 3.1415926535 zaokrouhlete na 4.

3

3

Testy prvočíselnosti (3)

Rabin-Millerův test

Zvolíme náhodně p a spočítáme b a m tak, aby platilo: $p = 1 + 2^b m$, kde m musí být liché $\Rightarrow$

1. Vybereme náhodné liché $a < p$.
2. Nechť $j = 0$ a $z \leftarrow |a^m|_p$.
3. Když $z = 1 \Rightarrow p$ může být prvočíslem, k další iteraci
4. Dokud $z \neq p - 1 \wedge j \leq b - 2 \Rightarrow$ opakuj $z \leftarrow |z^2|_p, j \leftarrow j + 1$.
5. Když $z \neq p - 1 \Rightarrow p$ určitě není prvočíslo

- Zjednodušená verze testu na prvočíselnost doporučeného normou DSS.
- Pravděpodobnost průchodu složeného čísla testem jako prvočísla klesá rychleji než u předchozích testů
- O $\frac{3}{4}$ hodnot a lze tvrdit, že mohou vystupovat v roli svědků.
- Znamená to, že složené číslo nepronikne t testy častěji než s pravděpodobností 4^{-t}.

R. Lórencz (ČVUT FIT) Generování klíčů, Rabin-Millerův test, náhodn BI-BEZ, 2020, Předn. 9. 18 / 38

- $4^{-2} = 1/16 = 0,0625$ (93,75 %)
- $4^{-3} = 1/64 = 0,015625$ (98,4375 %)
- $4^{-4} = 1/256 = 0,004$ (99,6 %)
- $100 - 98,354 = 1,646$

Mějme N zpráv $(x_1, x_2, \ldots, x_N)$ generované s pravděpodobnostmi $P(x_i)$, kde $N > 0$. Rozhodněte o pravdivosti následujících tvrzení.

1

???

✔ – ✖ Entropii nelze vyjádřit a ani spočítat, protože neznáme samotné hodnoty zpráv.

✔ – ✖ Nemůže nastat případ, kde entropie je rovna 0.

✔ – ✖ Pokud m zpráv má pravděpodobnost p_1 a $(N - m)$ zpráv pravděpodobnost p_2, pak entropie je rovna $-(m \cdot p_1 \cdot log_2(p_1) + (N - m) \cdot p_2 \cdot log_2(p_2))$.

✔ – ✖ Entropie je rovna $-\sum_{i=1}^{N} x_i \cdot log_2(P(x_i))$.

Jaký nejmenší exponent, a kolik mocnin nejvýše potřebujeme spočítat pro Rabinův-Millerův test čísla 481? Odpovědí jsou dvě čísla oddělená čárkou.

0

5,4

V pohádkovém království žije drak, jehož jídelníček obsahuje vyváženou stravu. Každé z jídel si může vybrat s určitou pravděpodobností uvedenou v závorce. Seznam jídel je následující: místní pobuda $\left(p_1 = \frac{1}{4}\right)$, běžný trpaslík $\left(p_2 = \frac{1}{4}\right)$, trpaslík s čepičkou $\left(p_3 = \frac{1}{4}\right)$, Červená Karkulka $\left(p_4 = \frac{1}{8}\right)$, potulný rytíř $\left(p_5 = \frac{1}{16}\right)$ a Hloupý Honza $\left(p_6 = \frac{1}{16}\right)$. Jaká je celková entropie drakova jídelníčku?

3

2.375

Definice – Entropie

Entropie je množství informace obsažené ve zprávě.
Teorie informace měří entropii zprávy průměrným počtem bitů nezbytných k jejímu zakódování při optimálním kódování (minimum bitů).

Entropie zprávy ze zdroje X je

$$H(X) = -\sum_{i=1}^{n} p_i \log_2 p_i,$$

$p_1, \ldots, p_n$ jsou pravděpodobnosti všech zpráv $X_1, \ldots, X_n$ zdroje X a $-p_i \log_2 p_i$ = # bitů nutných k optimálnímu zakódování zprávy X_i.

$= 2/16 \cdot \log_2(1/16)$
$+ 3/4 \cdot \log_2(1/4)$
$+ 1/8 \cdot \log_2(1/8)$
$= 2,375$

Označme h jako hashovací funkci SHA-384. Chceme nalézt dvě různé zprávy x_1 a x_2 takové, že $h(x_1) = h(x_2)$. Rozhodněte o platnosti následujících tvrzení:

3

✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{383}.

✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{192}.

✔ – ✖ Jedná se o kolizi druhého řádu.

✔ – ✖ Jedná se o kolizi prvního řádu.

Vypočítejte X_5 dané generátorem Blum-Blum-Shub. Koeficienty generátoru jsou: $p = 3, q = 11$. Seed X_0 je roven číslu 2.

3

4

Blum-Blum-Shub PRNG (1)

Příkladem PRNG, u kterého se má za to, že je kryptograficky bezpečný, je algoritmus Blum-Blum-Shub:

$$X_{n+1} = X_n^2 \bmod m \quad (2)$$

Modul $m = pq$ je součinem dvou velkých prvočísel p a q. Počáteční prvek (*seed*) je $X_0 > 1$. Mělo by platit, že $p, q \equiv 3 \pmod 4$, a $\gcd(\phi(p-1), \phi(q-1))$ by měl být malý.

Výstupem zpravidla není přímo hodnota X_n, ale její parita nebo několik nejméně významných bitů.

Vlastnosti:

- Pomalý
- Poměrně silný důkaz bezpečnosti (spojuje ji s výpočetní náročností faktorizace celých čísel)
- Lze přímo spočítat i-tý prvek posloupnosti:

$$X_i = (X_0^{2^i \bmod (p-1)(q-1)}) \bmod m \quad (3)$$

- $m = p \cdot q = 33$
- $X_1 = 2^2 \% 33$
- $X_2 = 4^2 \% 33$
- $X_3 = 16^2 \% 33$
- $X_4 = 25^2 \% 33$
- $X_5 = 31^2 \% 33 = 4$

Zvolili jsme prvočísla $p = 7, q = 13$ a veřejný exponent $e = 5$. Spočítejte soukromý exponent d, a zašifrujte zprávu $x = 3$. Odpovědí je modul n, soukromý exponent d a šifrový text c ve formátu 3 čísel oddělených čárkami. Příklad odpovědi: 1,2,3

3

91,29,61

- $n = p \cdot q = 91$
  - $\phi(n) = 72$
- $d = |e^{-1}|_{\phi n} = 29$
- $c = |x^e|_n = 61$

Pro zrychlení výpočtu u RSA používáme následující metody: 1

- ✔ – ✖ Čínskou větu o zbytcích
- ✔ – ✖ Krátký šifrovací exponent který má málo jedniček
- ✔ – ✖ Malý modul
- ✔ – ✖ Algoritmus Square&Multiply

2 2 2

Mějme posloupnost bitů 01111100100100 10 (0x7c92). Jaká bude výsledná posloupnost bitů po průchodu John von Neumannovým dekorelátorem?

3

0101

Vstup	Výstup
00, 11	– (vstup se zahodí)
01	0
10	1

Označme h jako hashovací funkci SHA-384. Chceme k dané zprávě x_1 nalézt zprávu x_2 různou od x_1 tak, že $h(x_1) = h(x_2)$. Rozhodněte o platnosti následujících tvrzení:

3

✔ – ✖ Jedná se o kolizi prvního řádu.

✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{96}.

✔ – ✖ Jedná se o kolizi druhého řádu.

✔ – ✖ Počet hashovacích operací (pro 50% pravděpodobnost) je zhruba 2^{192}.