1

První náhodná veličina neexistuje, protože kód není prefix-free, takže nemůže být Huffmanův. 10 je prefixem 101.

Druhá náhodná veličina také neexistuje, protože kód také není Huffmanův, jelikož není "nejlepší možný". Nemá tedy nejmenší možnou entropii, protože kód 110 by šel zkrátit na 11 a vše by fungovalo.

Třetí kódování již Huffmanovo je. Nechť kódujeme množinu $A = \{1, 2, 3, 4, 5\}$ Náhodná veličina X:

$a \in A$	1	2	3	4	5
Pr[X=a]	0,78	0,05	0,05	0,06	0,06
Kód	1	000	001	010	011

2

Nechť platí $\exists x, y \in \mathcal{C}, z \in \{0,1\}^* \setminus \epsilon : x = y||z$. Z definice Huffmanova kódování je y list ale x je z definice také list. Ale při dekódování x, bychom se dostali nejdříve do y (což je list) ale poté bychom nemohli již nikam pokračovat. Tedy by platilo, že $x = y$, což je ale spor, jelikož $z \neq \epsilon$.

3

Viz kód

4

$\Leftarrow$: Chceme dokázat, že latinský kryptosystém je absolutně bezpečný. Nechť $x \in \mathbb{P}, y \in \mathbb{C}, z \in \mathbb{K}$ a $\mathbf{P}, \mathbf{C}, \mathbf{K}$ příslušné náhodné veličiny, potom platí:

$$Pr(\mathbf{P} = x|\mathbf{C} = y) \overset{\text{def.}}{=} \frac{Pr(\mathbf{P} = x, \mathbf{C} = y)}{Pr(\mathbf{C} = y)}$$

Každý ciphertext je jednoznačně určen dvojicí (x, z) z toho, jak je definován latinský kryptosystém (jsou tam bijekce). Z toho plyne

$$Pr(\mathbf{P} = x, \mathbf{C} = y) = Pr(\mathbf{P} = x, \mathbf{K} = z) = Pr(\mathbf{P} = x) \cdot \frac{1}{n}$$

Poslední rovnost plyne také z definice lat. čtverce, jelikož znám-li z, mám řádek z n možnostmi. Dále $Pr(\mathbf{C} = y) = \frac{1}{n}$, jelikož čtverec obsahuje n^2 hodnot a z definice každá hodnota je stejněkrát. Tedy:

$$Pr(\mathbf{P} = x|\mathbf{C} = y) = \frac{Pr(\mathbf{P} = x) \cdot \frac{1}{n}}{\frac{1}{n}} = Pr(\mathbf{P} = x)$$

Tedy kryptosystém je absolutně bezpečný.

⇒: Chceme dokázat, že každý absolutně bezpečný kryptosystém je latinský čtverec. Dokážeme to sporem, tedy nechť kryptosystém není latinský čtverec. Uvažujme tabulku ciphertextů, kde řádek určuje plaintext a sloupec příslušný klíč. Z definice kryptosystému víme, že v žádném sloupci se hodnoty nesmí opakovat, jelikož bychom jedním klíčem zašifrovali 2 různé plaintexty na ten samý ciphertext.

Z předpokladu ale kryptosystém není latinský, tedy musí existovat alespoň jeden řádek, kde se hodnota alespoň jednou opakuje. Označme tuto hodnotu jako y. Jelikož y je v každém sloupci maximálně jednou a existuje řádek, kde je aspoň 2x, tak musí existovat řádek, ve kterém se y nenachází. To lze díky tomu že, množiny $\mathbb{P}, \mathbb{C}, \mathbb{K}$ mají stejnou mohutnost. Označme tento řádek (plaintext) jako x.

Poté platí $Pr(\mathbf{P} = x, \mathbf{C} = y) = 0$ ale $Pr(\mathbf{P} = x) \neq 0 \wedge Pr(\mathbf{P} = x) \neq 0$. Tedy

$$Pr(\mathbf{P} = x|\mathbf{C} = y) = \frac{0}{\neq 0} = 0 \neq Pr(\mathbf{P} = x)$$

Tedy kryptosystém není absolutně bezpečný ⇒ spor.

5