1

Řetězce pro 56 bitů (14 znaků v hex) jsou:
`JanOupicky309152359`
`JanOupicky172522389`
a příslušné SHA256 hashe:
`38852C61EE708A5B14663408662333E92D28E56133F060A1E729EDE96CDE6544`
`38852C61EE708A415601ED5E8B33081E2D0B7257B89ABDB8FAF5E16629C4DC78`

2

Viz soubor `uloha2.py`. Klíč je `0x3412`.

3

Nechť $j_k, i_k, S[j_k]$ značí hodnoty $i, j, S[j]$ na počátku smyčky v k. kroku. Počítáme v $\mathbb{Z}_{256}$. Platí tedy $j_k = i_k + 1$ a $S[j_k] = S[i_k + 1] = 1$. Potom:

$$i_{k+1} = i_k + 1$$

$$j_{k+1} = j_k + S[i_{k+1}] = j_k + S[i_k + 1]$$

$$S[i_k + 1] = 1 \Rightarrow \; j_{k+1} = j_k + 1$$

$$j_k = i_k + 1 = i_{k+1} \Rightarrow j_{k+1} = i_{k+1} + 1$$

$$S[j_{k+1}] \overset{\text{prohození}}{=} S[i_{k+1}] = S[i_k + 1] = 1$$

Tedy platí podmínky Finneyova stavu pro $k + 1$. krok.

4

Nechť Finneyův stav někdy nastane. Položme $k \geq 1$ (v 0. kroku je $i_0 = 0 \wedge j_0 = 0$, tedy nenastane Finneyův stav) první krok kdy Finneyův stav nastal (z předchozí úlohy víme, že takové k existuje). Dokážeme, že v tom případě musel nastat i v $k - 1$. kroku $\Rightarrow$ spor s minimalitou k.

Zase počítáme v $\mathbb{Z}_{256}$.

Máme tedy $j_k = i_k + 1 \wedge S[j_k] = S[i_k + 1] = 1$. Víme, že v předchozím kroku nastalo: $j_k = j_{k-1} + S[i_k]$. Dále víme, že $S[i_k]$ se prohodilo s $S[j_k] = 1$, tedy $S[i_k] = 1$ taktéž.

Dále $i_k + 1 = j_k = j_{k-1} + S[i_k] = j_{k-1} + 1 \Rightarrow i_k = j_{k-1}$. Z definice $i_k = i_{k-1} + 1 \Rightarrow j_{k-1} = i_{k-1} + 1$. A také $S[j_{k-1}] = S[i_k] = 1$. Takže i v

$k-1$. kroku nastal Finneyův stav $\Rightarrow$ spor viz výše. Tedy Finneyův stav nikdy nemůže nastat.

5

Ukážeme, že z kolize (x,y) pro h (tedy $x \neq y$) lze sestrojit kolizi pro f (obměněná implikace).
Nechť $x = M_1||\cdots||M_n$, $y = N_1||\cdots||N_k$, $x' = M'_1||\cdots||M'_{n+1}$ a $y' = N'_1||\cdots||N'_{k+1}$. Dále označme mezistavy pro x jako $S_0, S_1, \cdots, S_{n+1}$ a stavy pro y jako $T_0, T_1, \cdots, T_{k+1}$ kde $k, n \in \mathbb{N}$. Nakonec q přísluší x a q' přísluší y.

Předpokládáme, že:

$$h(x) = h(y) \iff S_{n+1} = T_{k+1} \iff f(S_n, M'_{n+1}) = f(T_k, N'_{k+1})$$

Takže buď $S_n \neq T_k \vee M'_{n+1} \neq N'_{k+1}$ a tím pádem máme kolizi pro f (hotovo), nebo $S_n = T_k \wedge M'_{n+1} = N'_{k+1}$. Předpokládejme tedy, že platí $S_n = T_k \wedge M'_{n+1} = N'_{k+1}$, potom platí:

$$[(M'_{n+1} = N'_{k+1}) \wedge (M'_{n+1} = 1||d-q) \wedge (N'_{k+1} = 1||d-q')] \Rightarrow \; q = q'$$

Takže víme, že $q = q'$. Pokračujeme dále:

$$S_n = T_k \iff f(S_{n-1}, M'_n) = f(T_{k-1}, N'_k)$$

Tedy zase buď máme kolizi pro f (hotovo), nebo $S_{n-1} = T_{k-1} \wedge M'_n = N'_k$. Pokračujeme stejně:

$$[(M'_n = 1||M_n||0^{d-q}) \wedge (N'_k = 1||N_k||0^{d-q})] \Rightarrow \; M_n = N_k$$

Pokud $k = n$, tak jistě existuje $i \in \{1, \cdots, n\}$ tž. $M'_i \neq N'_i$, protože $x \neq y$ $\Rightarrow$ kolize pro f.

Nebo BÚNO $k < n$. Pokud nenastane kolize pro $i \in \{2, \cdots, k\}$, tak z toho plyne $N'_1 = M'_{n-k+1}$, kde $N'_1 = (0||N_1) \wedge M'_{n-k+1} = (1||M_{n-k+1})$ což nemůže platit, protože se liší v prvním bitu.

Tedy spor, takže musela nastat kolize pro $i \in \{2, \cdots, k\}$, tedy kolize pro f. Takže f bezkolizní $\Rightarrow$ h je bezkolizní.

6