Kryptografia
Laboratorium nr 6

Stefan Sokołowski

Zadanie 1:

Porządna funkcja skrótu powinna

A. generować skróty zawsze tej samej długości; oraz

B. nie dawać możliwości obliczenia wiadomości z postaci skrótu; oraz

C. „praktycznie nigdy" nie produkować tego samego skrótu dla różnych wiadomości.

Poniżej podanych jest kilka naiwnie skonstruowanych funkcji skrótu. Proszę dla każdej z nich znaleźć ***wadę*** — uzasadnienie, że łamie ona któreś z wymagań **A** lub **B** lub **C**. Zakładamy, że wiadomości należą do zbioru $[1\,..\,100]^*$, czyli że pojedyncza wiadomość jest ciągiem dowolnej długości liczb naturalnych między 1 a 100.

(a) $f : [1\,..\,100]^* \to [0\,..\,822]$

$$f(w_0\, w1\, \ldots\, w_{n-1}) \stackrel{\text{def}}{=} \left(n + \sum_{i=0}^{n-1} w_i \right) \bmod 823$$

— ciągowi liczb przyporządkowana jest ich suma powiększona o ich ilość i zredukowana modulo 823 (to jest liczba pierwsza).

(b) $f : [1\,..\,100]^* \to [0\,..\,822]$

$$f(w_0\, w1\, \ldots\, w_{n-1}) \stackrel{\text{def}}{=} \left(\sum_{i=0}^{n-1} (i+1) \cdot w_i \right) \bmod 823$$

— ciągowi liczb przyporządkowana jest suma zredukowana modulo 823, ale przed sumowaniem każda liczba jest mnożona przez swoje kolejne miejsce w ciągu (w numeracji od 1).

(c) $f : [1\,..\,100]^* \to [0\,..\,822]$

$$f(w_0\, w1\, \ldots\, w_{n-1}) \stackrel{\text{def}}{=} \left((w_{n-1})^{w_0} \cdot \prod_{i=1}^{n-1} (w_{i-1})^{w_i} \right) \bmod 823$$

— każdą liczbę w ciągu podnosimy do potęgi, w której wykładnikiem jest następna liczba w ciągu (a dla ostatniej wykładnikiem jest początkowa), te wszystkie potęgi mnożymy, a następnie redukujemy modulo 823.

(d) $f : [1\,..\,100]^* \to [0\,..\,822]$

$$f(w_0\, w1\, \ldots\, w_{n-1}) \stackrel{\text{def}}{=} \left(\sum_{i=1}^{n-1} g(w_{i-1}, w_i) \right) \bmod 823 \quad \text{gdzie} \quad g(w, v) \stackrel{\text{def}}{=} w \oplus (w/v)$$

— każdą liczbę XORujemy z jej ilorazem całkowitym przez liczbę następną i sumę takich liczb redukujemy modulo 823.
