Wstęp do bezpieczeństwa komputerowego

Lista C1, 20 III

Zadanie 1 Motywacja do zadania: MS Word/Excel, Key Recovery Attack on 802.11b WEP, CVE-2020-1472.

Przechwyciłaś/eś kilkanaście kryptogramów. Wiesz, że każdy z nich powstał jako rezultat szyfrowania wiadomości za pomocą szyfru strumieniowego. Co więcej, do szyfrowania każdej wiadomości wykorzystano ten sam klucz i IV, czyli:

$$c_i = \mathsf{Enc}(\mathsf{k}, \mathsf{m_i}) = (IV, m_i \oplus G(k, IV)$$

dla $i = 1 \dots l$, gdzie G jest generatorem bitów pseudolosowych, k jest kluczem.

Zaprojektuj program, który przyjmuje na wejściu l kryptogramów zaszyfrowanych za pomocą szyfru strumieniowego z tym samym kluczem. Na wyjściu program ma zwrócić teksty jawne.

Zastanów się od czego będzie zależeć skuteczność programu:

- długości kryptogramów,
- liczby kryptogramów dla $l = 1, 2, 3, 4, \dots$ (od jakiej wartości l, program zaczyna działać?)
- typu szyfru strumieniowego G (Salsa20, Sosemanuk, AES-CTR, ...)
- wykorzystanego kodowania znaków ASCII/UTF-8/ISO-8859-2?

Zadanie z listy **P2** polegać będzie na implementacji takiego programu.

Zadanie 2 Udowownij, że definicje 1, 2, 3 z wykładu 2 (przypomniane poniżej) są równoważne.

Zadanie 3 (a) Udowodnij, że *shift cipher* (szyfr Cezara z losowym przesunięciem) jest doskonale tajny jeżeli szyfrujemy pojedyńczy znak. (b) Udowodnij, ze *One time pad* jest doskonale tajny.

Zadanie 4 (a) Pokaż, że tryb szyfrowania CBC nie jest CPA-secure jeżeli IV jest przewidywalne dla adwersarza (zobacz: CWE-329). (b) Pokaż, że CBC-MAC jest podrabialny jeżeli zamiast $IV = 0^n$ wartość IV jest wybierana losowo.

Definition 1. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every messsage $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$ for which $P[C = c] > 0$:

$$P[M = m | C = c] = P[M = m].$$

Definition 2. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if and only if for every probability distribution over $\mathcal{M}$, every message $m \in \mathcal{M}$, and every ciphertext $c \in \mathcal{C}$:

$$P[C = c | M = m] = P[C = c].$$

Definition 3. An encryption scheme $(\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ over a message space $\mathcal{M}$ is **perfectly secret** if for every probability distribution over $\mathcal{M}$, every $m_0, m_1 \in \mathcal{M}$, and every $c \in \mathcal{C}$:

$$P[C = c | M = m_0] = P[C = c | M = m_1].$$

Definition 4. A function f is $\mathsf{negligible}$ if for every polynomial $p(\cdot)$ there exists an N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.