Kryptografia dla informatyków I, 2017/18 22.2.2018

Egzamin poprawkowy - zadania

Stefan Dziembowski MIM UW

Zadanie 1:

Oblicz

$$2^{18780} \bmod 19043.$$

Wskazówka: $19043 = 137 \cdot 139$.

Zadanie 2:

Niech $(\mathsf{Tag} : \mathcal{K} \times \mathcal{M} \to \mathcal{T}, \mathsf{Vrfy} : \mathcal{K} \times \mathcal{M} \times \mathcal{T} \to \{\mathsf{true}, \mathsf{false}\})$ i $(\mathsf{Tag}' : \mathcal{K} \times \mathcal{M} \to \mathcal{T}', \mathsf{Vrfy}' : \mathcal{K} \times \mathcal{M} \times \mathcal{T}' \to \{\mathsf{true}, \mathsf{false}\})$ będą bezpiecznymi schematami uwierzytelniania wiadomości (ang. *Message Authentication Codes*). Zdefiniujmy $(\mathsf{Tag}'' : \mathcal{K} \times \mathcal{M} \to \mathcal{T}'', \mathsf{Vrfy}'' : \mathcal{K} \times \mathcal{M} \times \mathcal{T}'' \to \{\mathsf{true}, \mathsf{false}\})$ (gdzie $\mathcal{T}'' = \mathcal{T} \times \mathcal{T}'$) jako:

- $\mathsf{Tag}''(k, m) := (\mathsf{Tag}(k, m), \mathsf{Tag}'(k, m))$ oraz
- $$\mathsf{Vrfy}''(k, m, (t, t')) := \begin{cases} \mathsf{true} & \text{if } \mathsf{Vrfy}(k, m, t) = \mathsf{Vrfy}'(k, m, t') = \mathsf{true} \\ \mathsf{false} & \text{w przeciwnym przypadku.} \end{cases}$$

Czy $(\mathsf{Tag}'', \mathsf{Vrfy}'')$ też jest zawsze bezpiecznym schematem uwierzytelniania wiadomości? W przypadku odowiedzi pozytywnej podaj dowód, a w przykład takich $(\mathsf{Tag}, \mathsf{Vrfy})$ oraz $(\mathsf{Tag}'', \mathsf{Vrfy}'')$, że ta implikacja nie zachodzi.