Kryptografia

Lista 3

Problem 1 Udowodnij, że istnieje Π schemat szyfrowania z kluczem prywatnym, który ma nierozróżnialne kryptogramy względem podglądania (względem eksperymentu $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}(n)$), ale nie posiada nierozróżnialnych kryptogramów w eksperymencie $\mathsf{PrivK}^{\mathsf{mult}}_{\mathcal{A},\Pi}(n)$.

Problem 2 Udowodnij, że żaden schemat szyfrowania $\Pi = \langle \mathsf{Gen}(), \mathsf{Enc}(), \mathsf{Dec}() \rangle$, dla którego funkcja $\mathsf{Enc}() : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$ jest deterministyczną funkcją klucza i wiadomości nie może być schematem, który jest odporny na attak CPA (chosen-plaintext attack).

Problem 3 Udowodnij, że tryb szyfrowania ECB nie jest CPA-secure, bez względu na to jaka funkcja zostanie wykorzystana.

Problem 4 Dla schematu RC4 pokaż, że prawdobieństwo, że drugi bajt wyjścia będzie równy 0 jest większe niż 1/256.

Problem 5 Załóżmy, że w schemacie RC4 adwersarz otrzymuje permutację, która powstaje na koniec fazy KSA. Pokaż, że KSA w RC4 nie generuje permutacji w sposób jednostajny. Podpowiedź: zbadaj znak permutacji (rozdział 4 w `https://arxiv.org/pdf/1709.02631.pdf`).