Assignment 1 (for the 3rd week)

**Problem.** Determine which of the following functions are negligible:
(1) $2^{-n/\log n+\sqrt{n}\log n}$, (2) $2^{-\log n}$, (3) $2^{-\log\log n}$, (4) $2^{-\log n-\log\log n}$, (5) $2^{-(\log n)^2}$,
(6) $2^{-(\log\log n)^2}$, (7) $2^{-\log n\log\log\log n}$, (8) $2^{-\log n-(\log\log n)^2-(\log\log\log n)^3}$,
(9) $2^{-\log n\log\log n/\log\log\log n}$, (10) $2^{-\log n\log\log\log n/\log\log n}$, (11) $2^{-\log n/(\log\log n)^2}$,
(12) $2^{-(\log n)^2/(\log\log n)^4}$, (13) $2^{-\log n(\log\log n)^2/(\log\log\log n)^3+\log n\log\log n\log\log\log n}$.

Web page: `http://web-int.u-aizu.ac.jp/~yodai/course/SEC/welcome.html`

Assignment 2 (for the 4th week)

**Problem.** Prove the following proposition (by providing an explicit description of an adversary).

**Proposition 1.** *Let $\mathcal{PE} = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an encryption scheme such that $\mathcal{E}$ is deterministic. Then $\mathcal{PE}$ is not secure in the sense of $IND\text{-}ATK$.*

Web page: `http://web-int.u-aizu.ac.jp/~yodai/course/SEC/welcome.html`

Assignment 3 (optional)

**Problem.** Prove the following theorem (by constructing $NM\text{-}ATK$ adversary directly from $SS\text{-}ATK$ adversary).

**Theorem 1.** *$NM\text{-}ATK \rightarrow SS\text{-}ATK$.*

Web page: `http://web-int.u-aizu.ac.jp/~yodai/course/SEC/welcome.html`