Homework 3

Due date: Wednesday, March 22nd 11:30 AM

Question 1 (10 points)

Let f be a length-preserving one-way function, and let $\mathtt{hc}$ be a hard-core predicate of f. Define G as $G(x) = f(x) \| \mathtt{hc}(x)$. Is G necessarily a pseudorandom generator? Justify your answer.

Question 2 (20 points)

Let $x \in \{0,1\}^n$ and denote $x_1, \ldots, x_n$ as the bits of x. Prove that if there exists a one-way function, then there exists a one-way function f such that for every i there is an algorithm $A_i\left(f(x)\right)$, which successfully predicts the i^{th} bit x_i of x with probability

$$\Pr_{x \leftarrow \{0,1\}^n}\left[A_i\left(f(x)\right) = x_i\right] \geq \frac{1}{2} + \frac{1}{2n} \ .$$

Question 3 (20 points)

Let $x = (x_1, \ldots, x_n) \in \{0,1\}^n$ and denote by $\bar{x} = (1 - x_1, \ldots, 1 - x_n)$ the bitwise complement of z. Show that for every secret key k and input x we have

$$DES_k(x) = \overline{DES_{\overline{k}}\left(\overline{x}\right)} \ .$$

Question 4 (25 points)

Fix $N \in \mathbb{N}$ such that $N, e \geq 1$ and $\mathtt{gcd}\left(e, \phi(N)\right) = 1$. Assume that there is an adversary A running in time t such that

$$\Pr\left[A\left(\left[x^e \mod N\right]\right) = x\right] \geq 0.01$$

where the probability is taken over the uniform choice of $x \in \mathbb{Z}_N^*$. Show how to construct an adversary A' with running time $t' = O\left(poly\left(t, \log_2 N\right)\right)$ such that

$$\Pr\left[A\left(\left[x^e \mod N\right]\right) = x\right] \geq 0.99 \ .$$

Hint: Use the fact that $y^{1/e} \cdot r = \left(y \cdot r^e\right)^{1/e} \mod N$. Here, $y^{1/e} = y^d \in \mathbb{Z}_N^*$ where d is a (secret) number such that $ed \equiv 1 \mod \phi(N)$. Also use the fact that, given $r \in \mathbb{Z}_N^*$, we can find a number r^{-1} such that $rr^{-1} = 1 \mod N$.

Question 5 (25 points)

Let $pk = (N, e = 7) \in \mathbb{N}$ such that $N, e \geq 1$ and $\texttt{gcd}\,(e, \phi(N)) = 1$ be the public-key for an RSA encryption scheme and let $n = \lceil \log_{256}(N) \rceil$. To convert a bit string $x = x_1, \ldots, x_t \in \{0,1\}^t$ with to an integer in $\mathbb{Z}_N$ we define $\mathbf{Int}\,(x) = \sum_{i=1}^{t} x_i 2^{t-i}$.

Let m be the message "Pay Alice the following amount from Bob's bank account (USD): 50" and let μ denote a customized character to byte mapping such that $\mu(0) = 0^8, \mu(1) = 0^7 1, \ldots, \mu(9) = 00001001$, while other characters like 'a' or 'B' are mapped to bytes outside the range $[00000000, 00001001]$. Given $m = c_1, \ldots, c_{|m|}$ let $\mu(m) = \mu(c_1) \| \ldots \| \mu(c_{|m|})$ denote an encoding of m in bits (here $|m|$ denotes the number of characters in the message m). Similarly, given a bit string $x = x_1, \ldots, x_t \in \{0,1\}^t$ let $\mathbf{Int}\,(x) = \sum_{i=1}^{t} x_i 2^{t-i}$. Suppose that Bob sends Alice $\sigma = \mathbf{Sign}_{sk}\,(m) = \mathbf{Int}\,(\mu(m))^d \mod N$. Show how Alice can produce a signature σ' for a message authorizing the bank to transfer more than \$50 (you may assume that $|m| < n - 20$). Assuming that Alice knows that Bob has \$750 million in his bank account how much money can Alice get from Bob?