ECS 227: Modern Cryptography
Homework 4

Phillip Rogaway

Out: 20 February 1996. Due: Tuesday, 5 March 1996

11. Let $\mathcal{RSA}$ be the trapdoor permutation generator described in class and in the notes. Let $\mathcal{RSA}'$ be defined the same way, except that the composite N must be a *Blum integer*—it is the product of primes p and q each congruent to $3 \bmod 4$. Which is the (apparently) "weaker" (better) assumption: the intractability of $\mathcal{RSA}$, or the intractability of $\mathcal{RSA}'$? Answer this by carefully formulating and proving an (exact) result relating these two assumptions.

12. Suppose I give you an oracle I that takes an input (N, e, y), and has the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 1% of the values $y \in \mathsf{Z}^*_N$, the oracle I finds an $x \in \mathsf{Z}^*_N$ such that $x^e \bmod N = y$. Use I to develop an efficient algorithm A that has the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 99% of the values $y \in \mathsf{Z}^*_N$, the oracle I finds an $x \in \mathsf{Z}^*_N$ such that $x^e \bmod N = y$. Count how many calls to I your algorithm requires. *Hint: "randomize" the points you work on.*

13. Suppose I give you an oracle J that takes an input (N, e, y, p), where $|N| = k$, and has the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 51% of the values $\langle y, p\rangle \in \mathsf{Z}^*_N \times \{0,1\}^k$, the oracle I computes $x \odot p$, where $x^e \bmod N = y$. Explain how to use J to construct an algorithm B with the following behavior: for every N which is the product of two distinct primes, for every $e \in \mathsf{Z}^*_{\varphi(N)}$, for 99% of the values $y \in \mathsf{Z}^*_N$, the oracle I finds an $x \in \mathsf{Z}^*_N$ such that $x^e \bmod N = y$. Count how many calls to J your algorithm requires. *Hint: use problem 12.*

14. Let $B(x) = x[1 \mathinner{..} m] \odot x[m+1 \mathinner{..} n-\delta]$, where $n = |x|$, $m = \lfloor n/2 \rfloor$, and $\delta = n \bmod 2$. Suppose there exists a one-way function, f'. Prove that there exists a one-way function, f, such that B is not a hard-core bit of f.