Solution

Cryptography – Questionnaire 6

Name: ______________________________

Matr.: ______________________________

Questions– 1P each= 5P

	true	false
If RSA (i.e. $f(x) = x^e \bmod N$ with modulus $N = pq$) is an OWF then computing a $z < N$ with $\mathsf{gcd}(z, N) > 1$ has to be hard.	☒	☐
Let $f : \mathbb{Z}_{77}^* \to \mathbb{Z}_{77}^*$ with $f(x) = x^{13} \bmod 77$ and $g : \mathbb{Z}_{77}^* \to \mathbb{Z}_{77}^*$ with $g(x) = x^{43} \bmod 77$. Then f and g define the same map.	☒	☐
If OWP with hard-core predicate exist then PRGs of variable stretch exist.	☒	☐
If $\mathcal{P} = \mathcal{NP}$ then there are no CPA-secure ES.	☒	☐
OWF exist if and only if CCA-secure ES exist.	☒	☐

"One-liners"–2P+2P+1P = 5P

Exercise 6.1 **2P**

Compute the *least* positive integer d such that $g(x) := x^d \bmod (5 \cdot 17)$ is the inverse of $f(x) := x^3 \bmod (5 \cdot 17)$.
Answer: $d = 3^{-1} \bmod \lambda(5 \cdot 17) = 3^{-1} \bmod 16 = 11$

Exercise 6.2 **2P**

Show (i.e. sketch the argument briefly) that $f_n : \{0,1\}^{42} \times \{0,1\}^n \to \{0,1\}^{(n+44)}$ defined as $f(x, y) = (x||0) \cdot (y||1)$ is *not* an OWF (the multiplication $\cdot$ is to be interpreted in $Z^*_{2^{(n+44)}}$).
Answer: Given $y = f_n(x_1, x_2)$ we can simply enumerate all elements of $\{0,1\}^{42}$ (these are *finitely many* so it takes constant time :)) and try to divide y by each of these elements. If one such division succeeds (i.e. we get no remainder) we have found pre-images a, b with $f_n(a, b) = y$. Note that the runtime is polynomial in n as division of n bit numbers can be carried out in polynomial time and we do a *constant* ($\leq 2^{42}$) number of divisions!

Exercise 6.3 **1P**

How many solutions does the quadratic equation $X^2 \equiv 1 \bmod 51$ have? (*Hint*: $51 = 3 \cdot 17$)
Answer: 4