University of Edinburgh		Fall 17-18
IMC		Kiayias
Coursework 24.10.2017	Name :	
Due on 15 November 2017	ID :	

1] (Finding the inverse)

i) Explain in your own words the *Euclidean algorithm*[1] for computing the greatest common divisor (`gcd`) of two numbers

ii) Write in detail the computation for $\texttt{gcd}(70, 42)$.

iii) Explain in your own words how you can use the *extended* Euclidean algorithm[2] to compute the inverse of a number in a prime field.

iv) Write in detail the computation of the inverse of 476 in $\mathbb{F}_{7853}$.

2] (Statistical distance)

i) Let g be the generator of a cyclic group of prime order $m \in \omega(poly(\lambda))$, where λ is the security parameter. Compute the statistical distance of the random variables

$$D = \{x, y \xleftarrow{r} \{0, 1, \ldots, m\} : g^{xy}\} \text{ and } U = \{z \xleftarrow{r} \mathbb{Z}_m : g^z\}$$

ii) Let $D_1, \ldots, D_k$ be i.i.d random variables distributed according to D and $U_1, \ldots, U_k$ be i.i.d random variables distributed according to U. Show that:

$$\Delta[(D_1, \ldots, D_k), (U_1, \ldots, U_k)] \leq k \cdot \Delta[D, U]$$

iii) For what choices of k as a function of λ the statistical distance is negligible? (you can use asymptotic notation to express the functions in your answer)

[1] http://shoup.net/ntb/, Version 2, section 4.1
[2] http://shoup.net/ntb/, Version 2, section 4.2, 4.3