Homework 3

Encryption
Botond Lajos Perényi

Task 1: RSA cryptosystem

The paper claims that with having $\phi(n)$ it is trivial to break RSA. But it does not tell anything about how one might gain $\phi(n)$, which is not easy for large numbers, that are generally used with RSA. Finding the Totient function ($\phi(n)$) generally requires to calculate all the primes that are smaller than n, which is a time consuming task.
My advice based on this paper alone would be to keep using the already existing encryption system.

Task 2: Security definitions

Task 3: ElGamal encryption

Task 4: Attack on RSA encryption

Task 5: Choosing cryptographic primitives