

# Cryptography - Handin 5

---

Peter Burgaard - 201209175

October 13, 2016

## 1 EXERCISE 4

Suppose we are given a cryptosystem  $(G, E, D)$ . Assume an adversary develops an algorithm  $Alg$  running in time  $T$  that can take a ciphertext  $E_K(x)$  from an  $m$ -bit plaintext  $x$  and compute the first bit of  $x$ .

DESCRIBE AN ADVERSARY THAT PLAYS THE GAME IN THE CPA SECURITY DEFINITION AND USES  $Alg$  TO TRY TO DISTINGUISH THE REAL AND IDEAL CASE.

Since  $K$  is fixed for the entire attack, for our adversary to distinguish the real from the ideal case, he could feed the oracle the same input, and run the  $Alg$  repeatedly on each output, and if an output from  $Alg$  comes out with a different first bit than the others, the adversary would know he's in the ideal case due, to the fact that it would be a random string  $r$  being encrypted, and not a fixed message  $x$ . Of course the chance of each new  $r$  having the same first bit after iteration  $n$ , would be  $2^{-n}$  and by this method, the adversary would not be guaranteed a stop point in his effort to correctly figure out which case he's in.  
if same = real, og not = ideal

WHICH ADVANTAGE CAN YOU OBTAIN?

Since we can check when dealing with the real oracle if the output is correctly encrypted, and there's a 50% chance of the ideal oracle given us a message with the correct starting bit, our advantage would be

$$|1 - 0.5| = 0.5$$

IN TERMS OF THE PARAMETERS  $(t, q, \mu, \epsilon)$ , WHICH PARAMETER VALUES DOES YOUR ADVERSARY OBTAIN?

Since our algorithm take time  $T$  to run,  $T = t$ . We only need on call to make our decision which implies  $q = 1$ . Since the text string we send to the oracle is of length  $m$ ,  $\mu = m$ . And since we have advantage 0.5, this means  $\epsilon \geq 0.5$ .

HOW WOULD YOUR RESULT CHANGE IF  $Alg$  CANNOT COMPUTE THE FIRST BIT WITH CERTAINTY BUT ONLY GUESS IT WITH PROBABILITY  $p > \frac{1}{2}$ ?

$$P(R,R) = P(R,I) = 0.5p + (1-p) \cdot 0.5 = -0.5 \text{ Adv}(r,I) = p - 0.5$$