AARHUS UNIVERSITET, SCIENCE, COMPUTER SCIENCE

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 $E_K(x)$ form 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 cause 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.

So if the adversary is naive he will make the choice after the first call, with a string x, and if the first bit is the same, then he will assume we are in the real scenario, and if not, the we are in the 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, μ, ϵ), which parameter values does your adversary obtain?

Since our algorithm take time T to run, $T = t$. We only need one 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 $p > \frac{1}{2}$?

The probability that the adversary thinks we are in the real scenario, with Alg is obviously given the real scenario is $P(Real, Real) = P$. The probability of the guessing real given Alg when we are in the ideal must be the chance of getting the correct bit back $0.5 \cdot P$, and getting the correct bit wrongly back $(1-p) * 0.5$, which means $P(Real, Ideal) = 0,5p + (1-p) * 0.5 = 0.5$. This means our new advantage is |P-0.5|.