ECS 227 — Modern Cryptography — Winter 2009

Phillip Rogaway

Out: 26 January 2009. Due: 09 February 2009.

3. (a) In class we informally defined the bit-commitment problem. Design a plausible bit-commitment scheme using a blockcipher that has n-bit keys and n-bit blocks. (b) Can you arrange that commitments are information-theoretically binding? That is, with high probability, there exists little or no chance that the party who commits to more than one string—even if he has unbounded computational power. (c) Can you arrange that commitments are information-theoretically private? That is, with high probability, there exists little or no chance that the party who receives a commitment can understand what has been committed to—even if he has unbounded computational power?

4. Consider mounting an exhaustive key-search attack on DES: you are given a known plaintext/ciphertext pair $(X, Y) = (X, \mathrm{DES}_K(X))$ produced using a random key K and you try all keys, in lexicographic order, until you find a first one, K', where $E_{K'}(X) = Y$. Estimate or compute the probability that you have found the *wrong* key, $K \neq K'$? Specify any assumptions that you make. Remember that $|K| = 56$ and $|X| = 64$.