

Homework 1

Lecturer: Sasha Boldyreva

Due: February 14, 2006

Recommended reading is Chapters 1-4 and 7 from the lecture notes of Bellare and Rogaway and the relevant sets of slides.

Problem 1.1, 10 points. Your boss at a security company wants your group to design a PRF whose input length is 192 bits and the output is at least 192 bits. You know that it is not a good idea to design a new block cipher from scratch, so you decide to make use of the AES whose input-output length is 128 bits. Your colleague suggests the following construction Func-192: for every 128-bit key K and 192-bit message M $\text{Func-192}_K(M) = \text{AES}_K(M_{1-128}) \parallel \text{AES}_K(M_{129-192} \parallel 0^{64})$. Here M_{n-m} denotes the corresponding bits of M , 0^{64} is the string of 64 zeros and \parallel is the concatenation sign. Convince your boss that it is not a secure construction, however. Present an attack, e.g. an adversary and its analysis that shows that AES-192 is not a PRF. Note that Func-192 is not a block cipher, but it should not matter for the analysis.

Problem 1.2, 10 points. Pick any secure (in the sense of IND-CPA) encryption scheme we saw (CBC\$, CTR\$, CTRC). Show that it is not IND-CCA secure, i.e. present an adversary and analyze its ind-cca-advantage.

Problem 1.3

(a) 15 points. Your boss now wants your group to design a MAC that is secure for messages whose length is variable, but multiple of 128 bits (e.g. 256 or 1024 bits, etc), since he knows that the CBC-MAC is secure for messages of fixed length only. Your colleague proposes the following construction CBC-MAC-V, that uses AES (with keys, inputs and outputs of 128 bits). To MAC M under key K compute $\text{CBC-MAC}_K(M \parallel |M|)$, where $|M|$ denotes the length of M in blocks written in 128 bits. Show that your colleague's design is not good, i.e. this MAC is completely insecure: break it with a constant number of queries (present an adversary and analyze its uf-cma advantage).

(b) 10 points. You are smart enough not to re-invent the wheel and decide to consult the existing work on the subject. It must be the case that cryptographers thought about this issue and designed something secure. Search the Internet for block-cipher based secure MACs whose message space allows for messages of variable length (it is OK if they should have the length multiple of a block-cipher block length.) You may find the constructions that do not use block ciphers. You may recommend those to you boss (and me) as well, but you know that he wanted a block-cipher based construction for some reason. Provide detailed references and the names of

the constructions you found. The references have to contain the MACs' descriptions.
Make sure they were proven secure.