CS.202: Intro to Cryptography	Tuesday, 10/11/2016

Homework 3

Due Wednesday, 10/19/2016, at the beginning of the class

Notation: Let a and b be bitstrings. $a|b$ stands for the concatenation of a and b, $|a|$ stands for the bitlength of a, a_i stands for the i-th bit of a, $a_{[i,j]}$ for $i, j \in \{1, ..., |a|\}$ s.t. $i \leq j$ stands for a_L and a_R stand respectively for the substring of a from the i-th to the j-th bits of a, if a is even then a_L stands for $a_{[1,|a|/2]}$ and a_R stands for $a_{[|a|/2+1,|a|]}$.

1 Pseudorandom Generator Stretching Attempts

Let G be a PRG s.t. $|G(x)| = 2|x|$, e.g. G expands an ℓ-bit seed into a 2ℓ-bit string, for every input length ℓ. Below are attempts at using G to build H whose goal is to also be a PRG but with a larger expansion factor, i.e. $|H(x)| > |G(x)|$. For each attempt, state what is the expansion of H, i.e. $|H(x)|/|x|$, decide if H is secure for *every* PRG G, and prove your answer.

If your answer is positive, prove it. How? Probably by arguing a counterpositive, i.e. by showing that if there exists an efficient attack A against PRG security of H then you can show an efficient attack B which relies on algorithm A to attack PRG security of G.

And if your answer is negative, then exhibit it by providing an example of a particular PRG G which (1) is a secure PRG and (2) algorithm H using this G would become insecure as a PRG. In other words, G is a special-purpose PRG which you design to just show that H can be insecure for *some* PRG G. This is typically done by exhibiting a PRG G which has some special properties which are (1) not dangerous as far as PRG-ness of G is concerned, but (2) they make H insecure. How to show that there can exist a PRG G with such properties? Take any secure PRG $\bar{G}$ and try to construct G out of $\bar{G}$ so that G (1) G is a PRG if $\bar{G}$ is a PRG, but (2) G has a property that makes H not a PRG.

(a) Let $H(x) = G(1|x)$.

In other words, H runs a secure PRG G but not on fully random bitstrings but on bitstrings whose first bit is fixed as 1...

(b) Let $H(x) = G(x_L|x_R)|G(x_R|x_L)$ (assume ℓ is even).

In other words, run G twice, first on $x = x_L|x_R$ and then on $x' = x_R|x_L$, and output a concatenation of the outputs of G on these two strings.

(c) Let $H(x) = G(z_L)|G(z_R)$ where $z = G(x)$ is parsed as $z = z_L|z_R$.

In other words, run G to expand x into twice-longer string z and then apply G first to the left side of that string and then to its right side, and concatenate these.

2 PRG and Stream Cipher

We showed that if H is a PRG then a stream-cipher encryption which uses H for its key-generator, i.e. $E_k(m) = H(k) \oplus m$, is an indistinguishable encryption, a.k.a. it is semantically secure. (In this construction the keyspace is $K = \{0,1\}^{\ell}$ and message space is $M = \{0,1\}^{\ell'}$ where ℓ'/ℓ is the expansion factor of H.)

Show that the converse is also true, i.e. that if H is an insecure PRG then E is an insecure encryption. Show it by exhibiting an explicit attack B on the encryption indistinguishability of E given any attack A against the PRG property of H.

State what this implies about the security of stream cipher instantiated with each of the three constructions for H in problem 1.

3 CPA vs. Multiple-Message CPA (MM-CPA)

Recall the CPA security notion for encryption from the lecture (definition 3.22 in [KL]). Consider a seemingly stronger notion of encryption security, which we will call *Multiple-Message CPA Security*, defined in definition 3.23 in [KL]. Namely, the adversary A can adaptively choose pairs (m_0^i, m_1^i) of messages for $i = 1, ..., p(n)$ for any polynomial p and n the security parameter, with the only constraint that $|m_0^i| = |m_1^i|$ for every i. Each time A receives reply $c^i = E_k(m_b^i)$, where bit b is the challenger's bit, chosen at random at the beginning of the interaction.

Show that CPA security of E implies MM-CPA security of E. (This will show that the MM-CPA security notion is not stronger than CPA security: It is implied by it.)

Hint: Show that if there exists an efficient A which breaks MM-CPA of E then you can use this A to construct A' which breaks CPA security of E. You can do this considering a hybrid of distributions $D_0, ..., D_{p(n)}$ ms.t. D_0 corresponds to the view of A in the MM-CPA security game for $b = 0$, $D_{p(n)}$ corresponds to the view of A in the MM-CPA security game for $b = 1$, and for every i the only difference between D_i and D_{i-1} is how the challenger replies to A's i-th query (m_0^i, m_1^i)... If you can design such sequence of "hybrid" distributions between MM-CPA game on $b = 0$ and MM-CPA game on $b = 1$ then, by a hybrid argument, you will get that if A distinguishes between D_0 and $D_{p(n)}$ with non-negligible probability ϵ_A, then there must exist i s.t. A distinguishes between D_i and D_{i-1} with a (non-negligible) probability $\epsilon'_A = \epsilon_A/p(n)$. If distribution D_i is designed so that D_i and D_{i-1} differ on a *single* ciphertext, then perhaps you can construct an explit attack A' wich uses A to break the CPA security of E with advantage ϵ'_A because in the CPA security game the challenger's hidden bit b also acts on only a *single* ciphertext?