ICS 180: Introduction to Cryptography 6/03/2004

Homework 6

Due **Thursday**, *6/10/2004*

1 Symmetric encryptions from a PRP

Let $P : \{0,1\}^\tau \times \{0,1\}^m \to \{0,1\}^m$ be a PRP. Assume that m is polynomial in τ. Assume that every PPT adversary running in time t has at most advantage ϵ in distinguishing P from a random permutation, i.e. that for all PPT's A s.t. $Time_A \leq t$,

$$\mid Prob[A^{P_s}(1^\tau) = 1]_{s \leftarrow \{0,1\}^\tau} - Prob[A^R(1^\tau) = 1]_{R \leftarrow \mathsf{RNDPRM}(\tau,m)} \mid \leq \epsilon$$

Consider the following symmetric encryption scheme: The secret key is $s \leftarrow \{0,1\}^\tau$. To encrypt a message $M \in \{0,1\}^m$, the sender picks $r \leftarrow \{0,1\}^{m/2}$, concatenates r and M, and computes the ciphertext as $c = P_s([r \mid M])$.

1.1

Show how to decrypt.

1.2

Consider the security of this scheme in the sense of indistinguishability. Bound the advantage ϵ' that an adversary A' running in time t' has in distinguishing random ciphertexts of any two messages $M_0, M_1 \in \{0,1\}^m$.

1.3

Consider the security of this scheme against a *chosen-message attack*. In other words, consider an adversary A' which, before deciding on two test messages $M_0, M_1 \in \{0,1\}^m$, asks for ciphertexts on any adaptively chosen messages $M^{(1)},...,M^{(p(\tau))} \in \{0,1\}^m$ of his choice.

Is this encryption secure against such attack? If so, bound the advantage that A', running in time t', has in this attack.

1.4

Consider the security of this scheme against a *lunchtime attack*. I.e., here the adversary has an additional capability (on top of the chosen-message attack capability) of asking *before* he chooses the test messages M_0, M_1 for decryptions on adaptively chosen ciphertexts $C^{(1)},...,C^{(p(\tau))}$ of his choice.

Again, is this encryption secure against such attack? If so, bound the advantage that A', running in time t', has in this attack.

1.5

In class we considered a PRF-based encryption $Enc_s(M) = [r \mid P_s(r) \oplus M]$, where r was randomly chosen as $r \leftarrow \{0,1\}^m$.

Can you compare the two schemes in terms of their ciphertext length, efficiency, the requirements on P, and the provable security bounds (i.e. the bounds on t', ϵ' that you can show)?

2 Feistel Transforms

Recall that in class we showed that a 3-layer Feistel Network $\mathcal{H}^{(\mathcal{F},3)}$, instantiated with a PRF family $\mathcal{F}$, implements a PRP. In other words, we showed that for every PPT adversary A, the advantage of A in distinguishing, having a function oracle access to it, between a 3-layer feistel network H_{f_1,f_2,f_3}, for f_1, f_2, f_3 chosen at random in $\mathcal{F}_\tau$, from a random permutation on 2τ-bit strings, is a negligible function of the security parameter τ. In other words, we showed that for every A,

$$\{A^H(1^\tau)\}_{H \leftarrow \mathcal{H}_\tau^{(\mathcal{F},3)}} \approx \{A^P(1^\tau)\}_{P \leftarrow \mathsf{RNDPRM}(2k)}$$

2.1

Show that a 2-layer Feistel Network $\mathcal{H}^{(\mathcal{F},2)}$, instantiated with a PRF family $\mathcal{F}_\tau$, fails to implement a PRP. In other words, show a PPT attack in which an adversary has a significant advantage in distinguishing, having an function oracle access to it, a 2-layer feistel network H_{f_1,f_2}, for f_1, f_2 chosen at random in $\mathcal{F}_\tau$, from a random permutation on 2τ-bit strings. In other words, show A s.t.

$$\{A^H(1^\tau)\}_{H \leftarrow \mathcal{H}_\tau^{(\mathcal{F},2)}} \not\approx \{A^P(1^\tau)\}_{P \leftarrow \mathsf{RNDPRM}(2\tau)}$$

2.2

Show that a 3-layer Feistel Network $\mathcal{H}^{(\mathcal{F},3)}$, instantiated with a PRF family $\mathcal{F}_\tau$, fails to implement a *Strong* PRP. In other words, show a PPT attack in which an adversary has a significant advantage in distinguishing, having an oracle access to *both* F *and* F^{-1}, between F being a 3-layer feistel network H_{f_1,f_2,f_3}, for f_1, f_2, f_3 chosen at random in $\mathcal{F}_\tau$, and F being a truly random permutation on 2τ-bit strings. In other words, show A s.t.

$$\{A^{H,H^{-1}}(1^\tau)\}_{H \leftarrow \mathcal{H}_\tau^{(\mathcal{F},3)}} \not\approx \{A^{P,P^{-1}}(1^\tau)\}_{P \leftarrow \mathsf{RNDPRM}(2\tau)}$$

2.3 [bonus]

Show that a 4-layer Feistel Network $\mathcal{H}^{(\mathcal{F},4)}$, instantiated with a PRF family $\mathcal{F}_\tau$, does implements a Strong PRP. In other words, show a that for every PPT A we have

$$\{A^{H,H^{-1}}(1^\tau)\}_{H \leftarrow \mathcal{H}_\tau^{(\mathcal{F},4)}} \approx \{A^{P,P^{-1}}(1^\tau)\}_{P \leftarrow \mathsf{RNDPRM}(2\tau)}$$