ECS 227 — Modern Cryptography — Winter 00
Problem Set 2

Phillip Rogaway

Out: 20 January 2000. Due: 1 February 2000.

1. **Learn a block-cipher definition close-up.** Implement any one of the five AES Round-2 finalists. Turn in your source code.

   (There is a pointer on the Web page to the documents that define the five algorithms. RC6 is the quickest algorithm to implement (implementing it should take less than an hour). Rijndal is said to be quite elegant, too (I haven't read its definition). MARS is said to be a pretty likely winner, but it's pretty complicated.)

2. **Properties of DES.** Prove the following properties about the algorithm of the Data Encryption Standard. (Let $\overline{X}$ denote the bitwise complement of X. Let $\mathbf{0} = 0^{56}$ be 56 zero bits, and let $\mathbf{1} = 1^{56}$ be 56 one-bits.)

   (a) $\mathrm{DES}_K(M) = \overline{\mathrm{DES}_{\overline{K}}(\overline{M})}$.

   (b) $\mathrm{DES}_{\mathbf{0}}(\mathrm{DES}_{\mathbf{0}}(M)) = M$ and $\mathrm{DES}_{\mathbf{1}}(\mathrm{DES}_{\mathbf{1}}(M)) = M$.

   (c) $\mathrm{DES}_{\mathbf{1}}(\mathrm{DES}_{\mathbf{0}}(\cdot)) = \overline{\mathrm{DES}_{\mathbf{0}}(\overline{\mathrm{DES}_{\mathbf{0}}}(\cdot))}$.

3. **Two ways of expressing advantage.** Let $E : \mathrm{Keys} \times \{0,1\}^n \to \{0,1\}^n$ be a function family. Let A be an adversary. Recall that

$$\mathrm{Adv}_E^{\mathrm{prf}}(A) \quad = \quad \Pr[K \stackrel{R}{\leftarrow} \mathrm{Keys} : \ A^{E_K(\cdot)} = 1] - \Pr[\rho \stackrel{R}{\leftarrow} \mathrm{Rand}(n,n) : \ A^{\rho(\cdot)} = 1] \ .$$

   Let

$$\begin{aligned} \mathrm{Adv}_E^{\mathrm{prf2}}(A) \quad = \quad & 2\Pr[b \leftarrow \{0,1\} \ ; \ \textbf{if } b = 0 \textbf{ then } K \stackrel{R}{\leftarrow} \mathrm{Keys}, \ f \leftarrow E_K(\cdot) \\ & \qquad \textbf{else } f \stackrel{R}{\leftarrow} \mathrm{Rand}(n,n) : \ A^{f(\cdot)} = b] - 1 \ . \end{aligned}$$

   Show that these two measures of advantage exactly coincide: $\mathrm{Adv}_E^{\mathrm{prf}}(A) = \mathrm{Adv}_E^{\mathrm{prf2}}(A)$.

   Remark: This is a much stronger sort of equivalence than we need to regard two security measures as equivalent: it would have been enough that for every adversary A there exists an adversary A' of similar resources to A such that $\mathrm{Adv}_E^{\mathrm{prf}}(A) \approx \mathrm{Adv}_E^{\mathrm{prf2}}(A')$; and for every adversary A' there exists an adversary A of similar resources to A' such that $\mathrm{Adv}_E^{\mathrm{prf}}(A) \approx \mathrm{Adv}_E^{\mathrm{prf2}}(A')$.