ECS 227 — Modern Cryptography — Winter 99
Problems 7–9

Phillip Rogaway

Out: 28 January 1999. Due: 11 February 1999.

4. Alternative formulation of real-or-random security. Previously assigned.

7. From PRG to OWF. In class we said that a PRG $g(x) : \{0,1\}^\ell \to \{0,1\}^L$ immediately yields a OWF f: just set $f(x) = g(x)$. Give a careful theorem statement and proof for this.

8. GGM Backwards. Consider doing the opposite of the GGM construction: starting from a PRG $g : \{0,1\}^\alpha \to \{0,1\}^{2\alpha}$, define a PRF $F : \{0,1\}^\alpha \times \{0,1\}^\alpha \to \{0,1\}^\alpha$ by setting $x_\varepsilon = x$, $x_{s0} = g(x_s)[1..\alpha]$, $x_{s1} = g(x_s)[\alpha+1..2\alpha]$, and $F_a(x) = x_a$. (In other words, x is at the root of the tree and a specifies the path.) Assume g is a good PRG. Does the above construction work to give a good PRF? Explain.

9. Strong PRPs. A strong PRP is syntactically the same as a PRP—it is a map $F : \{0,1\}^\alpha \times \{0,1\}^\beta \to \{0,1\}^\beta$— but in measuring adversarial advantage we provide the adversary D with an oracle both for the permutation *and for its inverse*: we want that for reasonable adversary D,

$$\mathrm{Adv}_D^{\mathrm{sprp}} \;=\; \Pr[a \leftarrow \{0,1\}^\alpha :\; D^{F_a(\cdot),F_a^{-1}(\cdot)} = 1] - \Pr[\pi \leftarrow \mathrm{Perm}_\beta :\; D^{\pi(\cdot),\pi^{-1}(\cdot)} = 1]$$

is small. Consider the three-round Feistel construction that we used to make a good PRP from a good PRF. Does it actually produce a (good) strong PRP from a (good) PRF?