Assignment 1

Course: CS219cr Fall 99

October 19, 1999

Problem 1 It is a bad idea to choose $p = 2^k + 1$ for discrete-log based protocols:

(a) Show you can compute the least significant bit (lsb) of x when you are given y, g such that $y = g^x$. [Hint: consider $y^{(p-1)/2}$].

(b) Show how to compute the second lsb. Show how to compute x.

Problem 2 If you could compute the lsb of x from $c = e_k(x)$ where $e_k()$ is the RSA encryption, then you could find x. [Hint: Establish and prove the relation;

$$half(c) = parity(c \ \times \ e_k(2) \ mod \ n)$$

$$paritya(c) = half(c \ \times \ e_k(2^{-1}) \ mod \ n),$$

where $parity(c)$ returns the lsb of x and $half(c)$ returns 0, or 1, depending on whether x is in the first or second half of the $[0, n-1]$ interval, respectively.]

Problem 3 Suppose everybody's RSA public exponent e is 3, but users use different moduli, which with high probability are pairwise relatively prime. Show that if you send the same msg x to 3 different users you compromised x.

Problem 4 Show that breaking the ElGamal pk encryption is equivalent to solving the Diffie-Hellman problem.

Problem 5 Consider the field of integers modulo prime p.

(a) Show that you can view the standard addition and multiplication of rational as operations in the field above. (This is an homeomorphism from the field of rationals to the field mod p).

(b) By the above we can do the Elliptic Curve operations viewing the curve $y^2 = x^3 + ax + b$ in the real x, y plan, and do addition of (rational points) of the curve by the geometric interpretation we have seen in class (connect the two points by a line, and take the reflection with respect to the x-axis of the third point that the line intersects the curve. Prove associativity for the special case $P + Q - Q$.