CS255: Cryptography and Computer Security **Winter 1999**

Assignment #2

Due: Wednesday, February 17th, 1999.

Problem 1 In this problem, we see why it is a really bad idea to choose $p = 2^k + 1$ for discrete-log based protocols: the discrete logarithm can be efficiently computed for such p.

A. Show how one can compute the least significant bit of the discrete log. That is, given $y = g^x$ (with x unknown), show how to determine whether x is even or odd by computing $y^{(p-1)/2}$. [Hint: what does the lsb of x say about y?]

B. If x is even, show how to compute the 2nd least significant bit of x. [Hint: generalize the computation in Part A.]

C. By generalizing part B., show how to compute x.

The fact that $p = 2^k + 1$ is inappropriate for crypto is unfortunate since arithmetic operations modulo such p can be made to be very fast.

Problem 2 To achieve fast encryption it is desirable to make the public exponent e in the RSA cryptosystem as small as possible. Consider the case when $e = 3$. Show that given the public key an attacker can easily recover the half-most-significant bits of the private exponent d. In other words, show that when N is n bits long, an attacker can recover the $n/2$ most significant bits of d just given the modulus N. Is this a sufficiently serious threat that $e = 3$ should not be used? (just state your opinion)

A. Since $ed = 1 \bmod \varphi(N)$ there exists an integer k such that $ed - k\varphi(N) = 1$. First show that when $e = 3$ we must have $k = 2$. Recall that d is in the range $0 < d < \varphi(N)$.

B. Next show that given k and N it is easy to construct a number $\hat{d}$ that is very close to d — sufficiently close so as to match d on the $n/2 - 4$ most significant bits (with very high probability).
Hint: Observe that since p and q are on the order of $\sqrt{N}$ we have that $\varphi(N)$ is very close to N.

Problem 3 Let's explore why in the RSA public key system each person has to be assigned a different modulus $N = pq$. Suppose we try to use the same modulus $N = pq$ for everyone. Each person is assigned a public exponent e_i and a private exponent d_i such that $e_i \cdot d_i = 1 \bmod \varphi(N)$. At first this appears to work fine: to encrypt a message to Bob, Alice computes $C = M^{e_{bob}}$ and sends C to Bob. An eavesdropper Eve, not knowing d_{bob} appears to be unable to decrypt C. Let's show that using e_{eve} and d_{eve} Eve can very easily decrypt C.

A. Show that given e_{eve} and d_{eve} Eve can obtain a multiple of $\varphi(N)$.

B. Show that given an integer multiple of $\varphi(N)$ Eve can easily recover Bob's private key d_{bob} from his public key e_{bob}.

C. Deduce that Eve can decrypt any message encrypted using the modulus N (at this point this should be obvious).

Problem 4 Suppose one uses a modulus p and a generator g of $\mathbb{Z}_p^*$ as parameters for the ElGamal public key system. Show that the system leaks one bit of information about the plaintext. Namely, given the public key and a ciphertext, an eavesdropper can learn the Legendre symbol of the plaintext.