University of Waterloo
Department of C&O

PhD Comprehensive Examination in Cryptography
Spring 2003
Examiners: A. Menezes and E. Teske

July 2, 2003
1:00 pm — 4:00 pm
MC 5158A
Instructions

Answer as many questions as you can. Complete answers are preferred over fragmented ones. Questions have equal value.

Questions

1. Chosen-plaintext attack on two-key Triple-DES
   Recall that DES is a block cipher with key space \( K = \{0,1\}^{56} \), plaintext space \( M = \{0,1\}^{64} \), and ciphertext space \( C = \{0,1\}^{64} \). Encryption for two-key Triple-DES is defined as follows:
   \[
   E_k(m) = \text{DES}_{k_1}(\text{DES}^{-1}_{k_2}(\text{DES}_{k_1}(m)))
   \]
   where \( k = (k_1, k_2) \), and \( k_1, k_2 \in \{0,1\}^{56} \) is the secret key. Design a chosen-plaintext attack on two-key Triple-DES that takes roughly \( 2^{56} \) steps. (A step is a DES encryption or decryption operation.) Provide an explanation of why your attack works, and a careful estimate of its space and time requirements. (Hint: your attack may need a lot of chosen plaintext/ciphertext pairs.)

2. Elementary number theory
   (a) Prove that if \( p = 2^m + 1 \) is prime, then \( m \) is a power of 2.
   (b) Suppose that \( p = 2^m + 1 \) is prime. Prove that any quadratic nonresidue is a generator of \( \mathbb{F}_p^* \).
   (c) Suppose that \( p = 2^m + 1 \) is prime. Prove that 5 is a generator of \( \mathbb{F}_p^* \), except in the case \( p = 5 \).

3. Partial key-exposure in RSA
   This exercise shows that if the encryption exponent in RSA is \( e = 3 \), then the left half of the bits of \( d \) can be very easily computed. (More precisely, the possible values for the left half of the bits can be narrowed to one or two.)
   Let \( n = pq \) where \( p \) and \( q \) are primes with \( 5 \leq p < q < 2p \). Let integers \( e \) and \( d \) satisfy \( 1 < e, d < \phi(n) \) and \( ed \equiv 1 \pmod{\phi(n)} \).
   (a) Prove that there exists an integer \( k \) satisfying \( ed - k\phi(n) = 1 \) and \( 1 \leq k < e \).
   (b) Let \( \tilde{d} = \lfloor \frac{kn+1}{e} \rfloor \). Prove that \( |\tilde{d} - d| < 3\sqrt{n} \).
   (c) Prove that if \( e = 3 \) then \( k = 2 \).

4. Diffie-Hellman problem
   This exercise shows that the hardness of the Diffie-Hellman problem does not depend on the choice of generator.
   Let \( G \) be a (cyclic) group of prime order \( n > 2 \), and let \( \alpha \) be a generator of \( G \). We assume that the group operation in \( G \) can be computed in polynomial time. Recall that the Diffie-Hellman problem for \( G \) with respect to \( \alpha \) (DHP\(_\alpha\)) is the following: given \( \alpha^a \) and \( \alpha^b \), compute \( \alpha^{ab} \). In this question, you are given a polynomial-time algorithm \( A \) which solves DHP\(_\alpha\).
   (a) Devise a polynomial-time algorithm which on input \( \alpha^a \) and a positive integer \( k \), outputs \( \alpha^{ak} \).
   (b) Devise a polynomial-time algorithm which on input \( \alpha^a \) (with \( a \not\equiv 1 \pmod{n} \)), outputs \( \alpha^{a^{-1}} \).
   (c) Let \( \beta \) be a generator of \( G \). Devise a polynomial-time algorithm for solving DHP\(_\beta\) (i.e., given \( \beta^a \) and \( \beta^b \), compute \( \beta^{ab} \)).
5. **Security of the basic ElGamal public-key encryption scheme**

Let $G$ be a (cyclic) group of prime order $n > 2$, and let $\alpha$ be a generator of $G$. We assume that the group operation in $G$ can be computed in polynomial time. Recall that the Diffie-Hellman problem for $G$ with respect to $\alpha$ (DHP$_{\alpha}$) is the following: given $\alpha^a$ and $\alpha^b$, compute $\alpha^{ab}$. The decision Diffie-Hellman problem for $G$ with respect to $\alpha$ (DDHP$_{\alpha}$) is the following: given $\alpha^a$, $\alpha^b$ and $\alpha^c$, decide whether $c \equiv ab \pmod{n}$.

In the basic ElGamal public-key encryption scheme, Alice's private key is an integer $a \in [1, n - 1]$, and her public key is $\beta = \alpha^a$. To encrypt a plaintext message $m \in G$ for Alice, Bob selects $k \in_R [1, n - 1]$, and sends the ciphertext $C = (\alpha^k, m\beta^k)$ to Alice.

In the following, we consider ciphertext-only attacks on the basic ElGamal public-key encryption scheme. The attacker has knowledge of the group parameters, Alice's public key $\beta$, and one or more ciphers.

(a) The ElGamal-decrypt problem is the following: Given a public key $\beta$ and a ciphertext $C$, compute the corresponding plaintext. Prove that the ElGamal-decrypt problem is polynomial-time equivalent to DHP$_{\alpha}$.

(b) Prove that the semantic security of the basic ElGamal public-key encryption scheme (under ciphertext-only attack) is polynomial-time equivalent to DDHP$_{\alpha}$.

(c) Is the basic ElGamal public-key encryption scheme semantically secure against chosen-ciphertext attacks? (Justify your answer.)

6. **Elliptic curves**

Let $q$ be a power of an odd prime, $q \equiv 2 \pmod{3}$.

(a) Prove that the mapping $x \mapsto x^3$ is a 1-1 map of $\mathbb{F}_q$ to itself.

(b) Consider the elliptic curve $E : y^2 = x^3 + b$ defined over $\mathbb{F}_q$. Prove that the number of points in $E(\mathbb{F}_q)$ is $q + 1$.

(c) Prove that $E(\mathbb{F}_q)$ is cyclic.