Homework #2

UC Davis Students: Due May 2, 1997 at 11:59PM
NTU Students: Due May 9, 1997 at 11:59PM

1. (*20 points*) Consider an affine substitution cipher using the transformation $f(a) = (ak_1 + k_0) \bmod 26$. We suspect that the plaintext letter A (0) corresponds to the ciphertext letter H (7), and the plaintext letter I (8) corresponds to the ciphertext letter V (21). Please break the cipher by solving for k_0 and k_1.
2. (*20 points*) Denote the bit-by-bit complement of a block x as $\overline{x}$. The *complementation property* says that if $c = \text{DES}_k(m)$, then $\overline{c} = \text{DES}_{\overline{k}}(\overline{m})$. Please prove that this property holds, and then explain how this property can be exploited in a chosen-plaintext attack to reduce the search effort by approximately 50%.
   Hint: Obtain the ciphertext for a plaintext m and its complement $\overline{m}$.
3. (*40 points*) A *weak key* is a self-inverse key; that is, if $c = \text{DES}_k(m)$ and $m = \text{DES}_k(c)$., k is a weak key. The DES has four weak keys (assuming the parity bits are ignored). Please derive them.
   Hint: The encipherment and decipherment algorithms are the same in these cases. Consider what this means with respect to the key schedules for the weak keys.
4. (*30 points*) An RSA system uses $n = 29893$, and one user's public key is $e = 12335$.
   a. Please encipher the message $M = 25776$.
   b. Please determine the private key d. corresponding to the user's public key, and prove it is correct by deciphering the ciphertext computed in part a.
5. (*20 points*)Consider an RSA system in which $p = 97$, $q = 109$, and $e = 865$. Please determine the ciphertext corresponding to the messages $M = 124$, $M = 506$, and $M = 321$.
6. (*20 points*)An *iteration attack* on the RSA cipher is one in which repeated encipherings of the ciphertext produce the plaintext. Consider the ciphertext $C = 3$, $n = 25$, and $e = 17$. Please show that this message can be broken with the iteration attack.
7. (*30 points*) Consider the Morris-Thompson password encipherment scheme. Assume the attacker has full access to a list of users and their corresponding password hashes.
   a. Which would be more beneficial to preventing the guessing of passwords, increasing the length of the password to 16 characters or increasing the size of the salt to 24 bits, assuming that the attacker is trying to guess a particular user's password? Please justify your answer.
   b. How would your answer change if the attacker were simply trying to guess *any* user's password on the target system? Please justify this answer too.
8. (*20 points*) Consider the information gathering stage of the Flaw Hypothesis Methodology. If you were writing a "security manual" for the commands and library functions for your computer system, what details would you place on each manual page that might help a penetration tester hypothesize flaws?

Extra Credit

9. If messages are enciphered using the RSA system, determined for the modulus $n = pq$ (where p and q) are primes, and the public key is e, then there are $(1 + \gcd(e-1,p-1))(1 + \gcd(e-1,q-1))$ messages that are unconcealable (*i.e.*, the ciphertext is the plaintext message itself). Please prove this theorem.
10. Consider the set of messages that are idempotent in the set Z_n (that is, $m^2 = m \bmod n$). Please prove that the ciphertexts corresponding to these messages in an RSA system with modulus n are the messages themselves, regardless of the choice of public key.