CS/ECE/MATH 435 PRACTICE FINAL - DEC 10, 2009

Nigel Boston

Directions. Partial credit will be awarded for partial answers that are correct and relevant. For full credit explanations are required. No calculators permitted. Write all answers on the sheets provided.

1. Give a one-sentence definition of each of the following:
(a) Ciphertext-only attack
(b) Chosen-plaintext attack
(c) Known-plaintext attack

2. Which of the attacks in question 1 is most powerful? Which is least powerful?

3. The Solitaire cipher featured in Neal Stephenson's Cryptonomicon used a shuffled deck of cards as a key. What is the key space for this cipher? Is it bigger or smaller than the key space for AES-128?

4. What chosen plaintext would you use to attack the Vigenere cipher? A ciphertext TQFEQ VNQXT QFEVL AVMSV LESYE UXIQR was produced by a Vigenere cipher. We overheard that the first letter of the key is A. Decrypt the message.

5. A message that is 200 bits long is encrypted with a one-time pad. How many trial decryptions are necessary for a brute-force attack on this message?

6. List two advantages of stream ciphers over block ciphers.

7. Which of the following are stream ciphers and which are block ciphers?
(a) DES
(b) AES

8. An RSA system has parameters n, p, q, e, and d. What parameters are public and what must be kept secret? How is RSA typically used to encrypt long messages?

9. A Diffie-Hellman key exchange between Alice and Bob uses parameters p, g, a, and b. What values may be public and what values must be secret? Compute the session key they produce if $p = 101, g = 2, a = 4, b = 10$.

10. The UNIX password scheme hashes a password by encrypting it with DES 1000 times. Why 1000? That is, what would be worse if it was encrypted 1 time? 1000000 times?

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX