CPE 645 Computer Network Security
Fall 2015
Mid-term # 1
Department of Electrical and Computer Engineering
The University of Alabama in Huntsville

1. (10 points) Consider the storage of data in encrypted form in a large database using AES. One record has a size of 16 bytes. Assume that the records are not related to one another. Which mode would be best suited and why?

2. (10 points) You have received the following cipher text which was encoded with a simple shift cipher:
   `xultpaajcxitltlxaarpjhtiwtgxktghidhipxciwtvgtpilpitghlxiwiwtxgqadds`.
   Perform an attack against the cipher based on a letter frequency count: How many letters do you have to identify through a frequency count to recover the key? What is the clear text?

3. (10 points) Find all integers n between $0 \leq n < m$ that are relatively prime to m for m = 4, 5, 9, 26. We denote the number of integers n which fulfill the condition by ϕ (m), e.g. ϕ (3) = 2. This function is called "Euler's totient function". What is ϕ (m) for m = 4, 5, 9, 26?

4. (15 points) A commercial file encryption program from the early 1990s used standard DES with 56 key bits. In those days, performing an exhaustive key search was considerably harder than nowadays, and thus the key length was sufficient for some applications. Unfortunately, the implementation of the key generation was flawed, which we are going to analyze. Assume that you can test 106 keys per second on a conventional PC.
   The key is generated from a password consisting of 8 characters. The key is a simple concatenation of the 8 ASCII characters, yielding 64 = 8 x 8 key bits. With the permutation PC−1 in the key schedule, the least significant bit (LSB) of each 8-bit character is ignored, yielding 56 key bits.
   1. What is the size of the key space if all 8 characters are randomly chosen 8-bit ASCII characters? How long does an average key search take with a single PC?
   2. How many key bits are used, if the 8 characters are randomly chosen 7-bit ASCII characters (i.e., the most significant bit is always zero)? How long does an average key search take with a single PC?

5. (10 points) Assume we perform a known-plaintext attack against DES with one pair of plaintext and cipher text. How many keys do we have to test in a worst-case scenario if we apply an exhaustive key search in a straightforward way? How many on average?

6. (15 points) For the following, we assume AES with 192-bit key length. Furthermore, let us assume an ASIC (Application Specific Integrated Circuit) which can check 3×10^7 keys per second. If we use

100,000 such ICs in parallel, how long does an average key search take? Compare this period of time with the age of the universe (approx. 10^{10} years).

7. (10 points) Consider AES with 128-bit block length and 128-bit key length. What is the output of the first round of AES if the plaintext consists of 128 ones, and the first sub-key (i.e., the first sub-key) also consists of 128 ones? Show your work.

8. (15 points) a) Addition in GF(2^4): Compute (A(x)+B(x)) mod P(x) in GF(2^4) using the irreducible polynomial P(x) = x^4 +x+1. What is the influence of the choice of the reduction polynomial on the computation?
   1. A(x) = x^2+1, B(x) = x^3+x^2+1
   2. A(x) = x^2+1, B(x) = x+1

   b) Multiplication in GF(2^4): Compute A(x).B(x) mod P(x) in GF(2^4) using the irreducible polynomial P(x) = x^4+x+1. What is the influence of the choice of the reduction polynomial on the computation?
   1. A(x) = x^2+1, B(x) = x^3+x^2+1
   2. A(x) = x^2+1, B(x) = x+1

9. (5 points) List important design considerations for a stream cipher.