ECE: Advanced Information and Network Security
Homework 1 solutions
Fall 2012

1. Suppose that $n = 7 \cdot 11$, write out all the numbers a such that $gcd(a, n) = 1$. Do you see a pattern? Can you extend this observation to more general $n = pq$ where p and q are prime numbers?

Answer: It is all numbers relatively prime to 7 and 11, so remove 7, 14, 21, etc. Similarly, remove multiples of p and q in the general case.

2. Suppose $E_K(M)$ is the DES encryption of a message M using the key K. We showed in Chapter 4, problem 4, that DES has the complementation property, namely that if $y = E_K(M)$ then $\overline{y} = E_{\overline{K}}(\overline{M})$, where $\overline{M}$ is the bit complement of M. That is, the bitwise complement of the key and the plaintext result in the bitwise complement of the DES ciphertext. Explain how an adversary can use this property in a brute force, chosen plaintext attack to reduce the expected number of keys that would be tried from 2^{55} to 2^{54}. (Hint: This is a tricky problem. Consider a chosen plaintext set of (M_1, C_1) and $(\overline{M_1}, C_2)$).

Let K be the key we wish to find. Use the hint. Then $C_1 = E_K(M_1)$ and $C_2 = E_K(\overline{M_1})$. Now, suppose we start a brute force attack by encrypting M_1 with different keys. If, when we use K_j we get $E_{K_j}(M_1) = C_1$ then we are done and the key we desire is $K = K_j$. However, when we use K_j we can eliminate another key. Here is how. If $E_{K_j}(M_1) = \overline{C_2}$ then we know (by complementation property) that $E_{\overline{K_j}}(\overline{M_1}) = C_2$. Hence, if this happens, we know the key is $\overline{K_j}$ since $\overline{K_j}$ would decrypt C_2 to get $\overline{M_1}$. We are effectively testing two keys for the price of one! Hence, the key space is cut in half and we only have to search an average of 2^{54}.

3. Caesar wants to arrange a secret meeting with Marc Anthony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext EVIRE. However, Anthony does not know the key, so he tries all possibilities. Where will he meet Caesar? (Hint: This is a trick question.)

Solution: Among the shifts of EVIRE, there are two words: arena and river. Therefore, Anthony cannot determine where to meet Caesar.

4. Suppose you encrypt using an affine cipher, then encrypt the encryption using another affine cipher (both are working mod 26). Is there any advantage to doing this, rather than using a single affine cipher? Why or why not?

Solution: Let $mx+n$ be one affine function and $ax+b$ be another. Applying the first then the second yields the function $a(mx+n)+b = (am)x+(an+b)$, which is an affine function. Therefore, successively encrypting with two affine functions is the same as encrypting with a single affine function. There is therefore no advantage of doing double encryption in this case. (Technical point: Since $\gcd(a, 26) = 1$ and $\gcd(m, 26) = 1$, it follows that $\gcd(am, 26) = 1$, so the affine function we obtained is still of the required form.)

5. Show that the decryption procedures given for the CBC and CFB modes actually perform the desired decryptions.

CBC: We have $D_K(C_j) \oplus C_{j-1} = D_K(E_K(P_j \oplus C_{j-1})) \oplus C_{j-1} = P_j \oplus C_{j-1} \oplus C_{j-1} = P_j$.

CFB: $C_j \oplus L_8(E_K(X_j)) = (P_j \oplus L_8(E_K(X_j))) \oplus L_8(E_K(X_j)) = P_j$.

6. Let $K = 111 \cdots 111$ be the DES key consisting of all 1s. Show that if $E_K(P) = C$, then $E_K(C) = P$, so encryption twice with this key returns the plaintext.

Solution: The keys K_1, . . . ,K_{16} are all the same (all 1s). Decryption is accomplished by reversing the order of the keys to K_{16}, . . . , K_1. Since the K_i are all the same, this is the same as encryption, so encrypting twice gives back the plaintext.