ECE Information and Network Security
Homework 1
Spring 2008

Chapter 2:

3. Changing the plaintext to numbers yields 7, 14, 22, 0, 17, 4, 24, 14, 20. Applying 5x+7 to each yields $5 \cdot 7 + 7 = 42 = 16 \pmod{26}$, $5 \cdot 14 + 7 = 77 = 25$, etc. Changing back to letters yields QZNHOBXZD as the ciphertext.

6. 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.)

7. For an affine cipher $mx + n \pmod{27}$, we must have gcd(27,m) = 1, and we can always take $1 \leq m \leq 27$. So we must exclude all multiples of 3, which leaves 18 possibilities for m. All 27 values of n are possible, so we have $18 \cdot 27 = 486$ keys. When we work mod 29, all values $1 \leq m \leq 28$ are allowed, so we have $28 \cdot 29 = 812$ keys.

23. The number of seconds in 120 years is

$$60 \times 60 \times 24 \times 365 \times 120 \approx 3.8 \times 10^9.$$

Therefore you need to count $10^{100}/(3.8 \times 10^9) \approx 2.6 \times 10^{90}$ numbers per second!

Chapter 3

1. (a) Apply the Euclidean algorithm to 17 and 101:

$$101 = 5 \cdot 17 + 16$$

$$17 = 1 \cdot 16 + 1.$$

Working back yields $1 = 17 - 16 = 17 - (101 - 5 \cdot 17) = (-1) \cdot 101 + 6 \cdot 17$.

(b) Since $-101 + 6 \cdot 17 = 1$, we have $6 \cdot 17 \equiv 1 \pmod{101}$. Therefore $17^{-1} \equiv 6 \pmod{101}$.

5. (a) $4883 = 1 \cdot 4369 + 514 \cdot 4369 = 8 \cdot 514 + 257 \cdot 514 = 2 \cdot 257 + 0$. Therefore, the gcd is 257. (b) We know that both numbers have 257 as a factor. This yields $4883 = 257 \cdot 19$ and $4369 = 257 \cdot 17$.

Chapter 4

1. (a) Switch left and right halves and use the same procedure as encryption. The switch the left and right of the final output. Verification is the same as that on pages 115-116.

(b, c) 1st round: $M_0M_1 \rightarrow M_1[M_0 \oplus K \oplus M_1]$

2nd round: $[M_0 \oplus K \oplus M_1][M_1 \oplus M_0 \oplus K \oplus M_1 \oplus K] = [M_0 \oplus K \oplus M_1][M_0]$

3rd round: $[M_0][M_0 \oplus K \oplus M_1 \oplus K \oplus M_0] = [M_0][M_1]$, which is the plaintext.

Therefore 3 rounds is very insecure! After 2 rounds, the ciphertext alone lets you determine M_0 and therefore $M_1 \oplus K$, but not M_1 or K individually. If you also know the plaintext, you know M_1 are therefore can deduce K.

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

5. (a) The keys $K_1, \cdots, K_{16}$ 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. (b) The key of all 0s , by the same reasoning.