ECE Information and Network Security
Homework 2
Spring 2008

Chapter 3:

2. 2. (a) Apply the Euclidean algorithm to 7 and 30:

$$30 = 4 \cdot 7 + 2$$

$$7 = 3 \cdot 2 + 1.$$

Working backwards yields $1 = 7 - 3cdot2 = 7 - 3 \cdot (30 - 4 \cdot 7) = 13 \cdot 7 + (-3) \cdot 30$. Therefore $13 \cdot 7 = 1 \pmod{30}$, so $d = 13$.

(b) Let $c = m^7 \pmod{31}$ be the ciphertext. Claim: $c^{13} = m \pmod{31}$. Proof: $c^{13} = (m^7)^{13} = m^{91} = (m^{30})^3 m$. If $m \neq 0 \pmod{31}$ then $m^{30} = 1 \pmod{31}$ by Fermat. Then $c^{13} = 1^{13} m = m$. If $m = 0 \pmod{31}$, then $c = m^7 = 0$, so $c^{13} = 0 = m$. Therefore $c^{13} = m$ for all m. Therefore decryption is performed by raising the ciphertext to the 13th power mod 31.

12. By Fermat's theorem, $2^{100} = 1 \pmod{101}$. Therefore, $2^{10203} = (2^{100})^{102} 2^3 = 1^{102} 2^3 = 8$. Therefore, the remainder is 8.

Chapter 6:

1. We have $\phi(n) = (p-1)(q-1) = 100 * 112 = 11200$. A quick calculation shows that $3 \equiv 7467^{-1} \pmod{11200}$. We have $5859^3 \equiv 1415 \pmod{11413}$, so the plaintext was $1415 = no$.

2. (a) Here $\phi(n) = 4 \cdot 10 = 40$. We are looking for a number d such that $ed = 1 \pmod{40}$. Thus, we want to solve for d in $3d = 1 \pmod{40}$. Observe that $d = 27$ gives $3 \cdot 27 = 81 = 1 \pmod{40}$. Hence $d = 27$.

(b) Here, you use Euler's Theorem. d is such that $3d = 1 + k\phi(n)$ for some k. Then, $c^d = m^{3d} = m^{1+k\phi(n)} = m \pmod{n}$ by Euler's Theorem.

8. We have $c_2 \equiv c_1^{e_2} \equiv m^{c_1 c_2} \pmod{n}$. Therefore, this double encryption is the same as single encryption with encryption exponent $e_1 e_2$. So the security is at the same level as single encryption.

12. We have $(516107 \cdot 187722)^2 \equiv (2 \cdot 7)^2 \pmod{n}$. Compute $\gcd(516107 \cdot 187722 - 2 \cdot 7, 642401) = 1129$. Therefore, $642401 = 1129 * 569$.

17. Make a list of 1^e, 2^e, ... , $26^e \pmod{n}$. For each block of ciphertext, look it up on the list and write down the corresponding letter. The message given is *hello*.