ECE Information and Network Security
Homework 3 solutions
Spring 2006

Chapter 6 problems

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, $642401 = 1129 * 569$.

23. The spy tells you that $m^{12345} \equiv 1 \pmod{n}$. Hence $\psi = 12345$ acts like $\phi(n)$ (in the sense of Euler's Theorem). Now, if we can find a δ such that $e\delta \equiv 1 \pmod{\psi}$, then we have that $e\delta = k\psi + 1$ for some k, and thus $c^\delta = m^{e\delta} = (m^\psi)^k m \pmod{n} = m$. Therefore, all that is needed to decrypt is to use the publicly available e and solve $e\delta = 1 \pmod{12345}$, and then use δ as the decryption exponent.

Supplemental Problem: How do you find the first 3 digit prime? Answer: We start by letting $n = 100$ and divide n by all whole numbers (besides 1) less than or equal to $\sqrt{n}$. If any of these divisions produces a remainder of 0, then we have found a factor. In this case, we increment $n = n+1$. Otherwise, if none of the divisions had a zero remainder, then we have found the first prime.