# ECE: Advanced Information and Network Security
# Homework 1
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?

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 $(\overline{M_1}, C_2)$).

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.)

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?

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

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.