# MATH 220
## Discrete Mathematics and Cryptography

**Tutorial 4** **Week starting 17 March 2020**

**1.** Calculate $\phi(1001)$ and $\phi(1000)$.

**2.** Show that, for any positive integers $n$ and $m$,

$$\phi(n^m) = n^{m-1}\phi(n).$$

*Hint.* Use the prime decomposition of $n$.

**3.** Use the previous question to calculate $\phi(1000)$ again.

**4.** Write 110 in binary notation and use fast exponentiation to calculate

$$9^{110} \bmod 19.$$

Check your result using Fermat's Little Theorem.

**5.** Find the discrete logarithm of each element in $\mathbb{Z}_{11}^*$ to the base 2. What would happen if you tried base 3?

**6.** An RSA cipher is set up with the public keys $n = 12091$ (the modulus) and $r = 3$ (the exponent). The plaintext is $m = 2107$.

(a) Encrypt $m$.

(b) Find the decryption key for the cipher.

(c) The ciphertext is $c = 9812$. Decrypt it.

**7.** Alice chooses primes $p = 149$ and $q = 317$, and encryption exponent $e = 71$. What public modulus does she publish? What is her decryption exponent?

**8.** Alice and Alicia each set up an RSA cryptosystem with the same modulus $n$, but different encryption exponents $e_1$ and $e_2$. Bob encrypts the same message, sending $c_1 \equiv m^{e_1} \bmod n$ to Alice and $c_2 \equiv m^{e_2} \bmod n$ to Alicia. If $e_1$ and $e_2$ are relatively prime, show that knowing $c_1$ and $c_2$ is sufficient for Eve to find $m$.

**9.** You and a friend are using the Rabin cipher system with $n = 713$ as your public key. You have received the ciphertext $c = 200$. What is the corresponding plaintext?

*Hint.* The result $13^2 \equiv 14 \bmod 31$ may be useful!

**10.** A Rabin cipher is set up with the public key $n = 65$. The plaintext message is $m = 17$.

(a) Show that $m$ is encrypted to $c = 29$.

(b) Decrypt the ciphertext $c = 29$ to find the four possible values of $m$.

**11.** Let $p$ and $q$ be primes, and let $n = pq$. Show that, for all $a, b \in \mathbb{Z}$, we have $a \equiv b \bmod n$ if and only if $a \equiv b \bmod p$ and $a \equiv b \bmod q$.

**12.** Let $p$ be a prime such that $p \equiv 3 \bmod 4$. Show that if $a$ is square $\bmod p$, then $x = a^{\frac{p+1}{4}}$ is a square root of $a \bmod p$. Why is $p - x$ also a square root of $a \bmod p$?

*Hint.* Use Fermat's Little Theorem.