MATH 233 SPRING 2018
FINAL PRACTICE PROBLEMS 1

MTH233 Cryptography Spring 2018 final will be at 8:30am in Hylan 102 on Tuesday May 8, 2018.

- **Calculators are allowed for doing arithmetic, not for looking up information. Computers, ipads, etc. are not allowed. The exam is closed book. You may bring one sheet of notes (you can write on both sides).**
- **Show your work and justify your answers. You may not receive full credit for a correct answer if insufficient work is shown or insufficient justification is given.**
- Honor pledge: "I affirm that I have not used, given nor received unauthorized aid during this examination and that all work is my own."

  Signature:

---

(1) (a) Let E_1 and E_2 denote encryption by Vignère ciphers, not necessarily with the same keywords. True or false and explain: we must have $E_1(E_2(m)) = E_2(E_1(m))$ for any plaintext m.
(b) Let E_3 and E_4 denote encryptions by Hill block ciphers of length 2, not necessarily the same Hill block ciphers. True or false and explain: we must have $E_3(E_4(m)) = E_4(E_3(m))$ for any plaintext m.
(c) Let E_5 be Vignère encryption with keyword be and E_6 be Vignère encryption with keyword $nrdn$. Encrypting first with E_5 and then with E_6 gives a Vignère with what keyword?

(2) Suppose we have an RSA encryption system with

$$n = 991 \cdot 607 = 601537.$$

(a) Suppose that the encryption exponent is $e = 17$. Find $d \pmod 4$, where d is the decryption exponent. (That is, find out what d is modulo 4.) [Hint: 4 divides $\phi(n)$.]
(b) Suppose that the encryption exponent is $e = 19$. Find $d \pmod 4$, where d is the decryption exponent. (That is, find out what d is modulo 4.)

(3) Given that $60^2 \equiv 1 \pmod{3599}$, give a factorization of 3599.

(4) Let $p = 1021$. Then $L_2(3) = 10$, that is $2^{10} \equiv 3 \pmod{1021}$.
(a) Find $L_2(9)$.
(b) Find $L_2(6)$.

(5) Using the RSA signature algorithm, Alice has $n = 33$ and $e = 3$ (that is, the RSA encryption here is $c \equiv m^3 \pmod{33}$). Which of the following pairs (m, m^d) (where d is her secret decryption exponent) has been signed by Alice?
(a) $(27, 3)$.
(b) $(11, 7)$.
(c) $(31, 4)$.

(6) Suppose that we have three DES keys K_1, K_2, and K_3 (each 56 bits). For each encryption method below, state how long it should take to find the break the encryption system (i.e. find the relevant keys), given that you know m and c. Explain whether you are using meet-in-the-middle and how you are using. (As usual E_{K_i} denotes DES encryption with the key E_{K_i}).
(a) $c = E_{K_1}(E_{K_2}(m))$.
(b) $c = E_{K_1}(E_{K_2}(E_{K_3}(m)))$.
(c) $c = E_{K_1}(E_{K_2}(E_{K_2}(m)))$.

(d) $c = E_{K_1}(E_{K_2}(E_{K_1}(m)))$.

(7) The hash function SHA-224 has 224 bit output. We denote the function as h (where $h(m)$ is SHA-224 applied to m for any m of length $2^{128} - 1$ or fewer bits). (You may assume that this hash function is only attackable by brute force attacks.)
   (a) About how long should it take to find some $m_1 \neq m_2$ such that $h(m_1) = h(m_2)$? (Explain your answer.)
   (b) Given a fixed m, about how long should it take to find some $m' \neq m$ such that that $h(m') = h(m)$? (Explain your answer.)

(8) Suppose we define a hash function by $h(m) = 3^m \pmod 7 + 7 \cdot (2^m \pmod{11})$. Find two integers $m_1 \neq m_2$ with $0 < m_1, m_2 < 32$ such that $h(m_1) = h(m_2)$.

(9) The purpose of this problem is to show that for any RSA set-up with $n = pq$, for $p \neq q$ both odd primes, that there are at least four choices of encryption exponent $e < (p-1)(q-1)$ such that $e^2 \equiv 1 \pmod{(p-1)(q-1)}$.
   (a) Let $m \geq 2$. Show that 1, $2^{m+1} - 1$, $2^m + 1$, and $2^m - 1$ are all distinct (no two are equal to each other) and that each satisfies $x^2 \equiv 1 \pmod{2^{m+1}}$.
   (b) Let $n > 1$ be any odd number. Show that there are at least 4 distinct positive integers $x < 2^2 n$ such that $x^2 \equiv 1 \pmod{2^2 n}$.
   (c) Let p and q be odd primes. Show that $(p-1)(q-1)$ is divisible by 4.
   (d) Let p and q be any odd primes with $p \neq q$. Show that there are at least 4 distinct positive integers $e < (p-1)(q-1)$ such that $e^2 \equiv 1 \pmod{(p-1)(q-1)}$. [Hint: Let 2^{m+1} be the highest power of 2 that divides $(p-1)(q-1)$. Show that if $m+1 \leq 2$, then $(p-1)(q-1)$ must have an odd prime factor.]

(10) Using the following facts:
   $(i, 3^i \pmod{31}), i = 0 \ldots 6$ is $[(0,1),(1,3),(2,9),(3,27),(4,19),(5,26)]$
   $(i, 11 * 3^{-i*6} \pmod{31}), i = 0 \ldots 11 [(0,11),(1,22),(2,13),(3,26),(4,21),(5,11)]$
   calculate $x = Log_3(11)$ where $0 \leq x < 30$. 3 is a primitive root of 31.
   Why was 6 the appropriate number to use in constructing the list above?

(11) Find the inverse of a polynomial in a finite field.
   Let $GF = \{a_0 + a_1 X + a_2 X^2 + a_3 X^3 + \cdots \mid \pmod{X^4 + X^2 + X + 1}\}$
   $X^4 + X^2 + X + 1$ is an irreducible polynomial.
   Find the inverse of $g = X + 1$ in this field.

(12) Set $p = 601$ (a prime).
   (a) Define the properties of a primitive root α mod p.
   A primitive root (or generator) has the property that α^k maps onto all of the invertible elements mod p hence $\alpha^k \equiv 1$ iff $k = p - 1$ and using fermat's theorem $\alpha^{(p-1)/2} \equiv -1$
   (b) Note that $600 = 2^3 \cdot 3 \cdot 5^2$. Assume also that a calculation shows that
   $7^{300} \equiv 600, 7^{200} \equiv 576, 7^{120} \equiv 423 \pmod{601}$
   Show that 7 must be a primitive root mod 601.

(13)
   (a) Compute $6^5 \pmod{11}$.
   (b)Let $p = 11$. Then 2 is a primitive root. Suppose that $2^x \equiv 6 \pmod{11}$ Without finding the value of x determine whether x is even or odd.