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?

Solution:

Solution:

(a) This is true: By repeating the keywords if necessary, we can assume that the keys K_1 and K_2 for E_1 and E_2, respectively, have the same length. (For example, if K_1 has length 2 and K_2 has length 3, then we could repeat K_1 three times and K_2 twice to get two keywords of length six.) Then the keyword for $E_1 \circ E_2$ is $K_2 + K_1 \pmod{26}$ and the keyword for $E_2 \circ E_1$ is $K_1 + K_2 \pmod{26}$, and the two are the same since addition mod 26 is commutative.

(b) This is false: Let E_3 and E_4 be encryption using the matrices

$$M_3 = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \text{ and } M_4 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Let $m = (1, 0)$. Then

$$E_3(E_4(m)) = mM_4M_3 = (1,0) \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = (2,1),$$

but

$$E_4(E_3(m)) = mM_3M_4 = (1,0) \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = (1,1).$$

Note: The reason the order doesn't matter for (a) is that addition mod 26 is commutative, and the reason order does matter for (b) is that matrix multiplication is not commutative.

(c) The keyword `be` corresponds to $(1, 4)$ and `nrdn` corresponds to $(13, 17, 3, 13)$, so the keyword for the double encryption is

$$(1,4,1,4) + (13,17,3,13) \equiv (14,21,4,17) \pmod{26},$$

which corresponds to the keyword `over`. (Note that we repeated `be` twice and only repeated `nrdn` once.)

□

(2) An affine-like cipher given by $c \equiv \alpha x + \beta \pmod{26}$ (where c is the cipher and x is plaintext) encrypts the plaintext *abe* as *ben*. Is *abe* the *only* three letter text that is encrypted as *ben* by this affine-like cipher? If "yes", explain why. If "no", then provide another example of plaintext that enrcrypts as *ben* under this affine-like cipher.

Solution:

Solution: Since `abe` is encrypted to `ben`, we have

$$0 \mapsto 1, \ 1 \mapsto 4, \ 4 \mapsto 13.$$

Let $f(x) = ax + b$ be the affine encryption function. Then

$$f(0) \equiv 1 \pmod{26} \implies a \cdot 0 + b \equiv 1 \pmod{26} \implies b \equiv 1 \pmod{26}.$$

We also have

$$f(1) \equiv 4 \pmod{26} \implies a \cdot 1 + b \equiv 4 \pmod{26} \implies a + 1 \equiv 4 \pmod{26} \implies a \equiv 3 \pmod{26}.$$

Therefore $f(x) \equiv 3x + 1 \pmod{26}$. Since $\gcd(3, 26) = 1$, 3 is invertible mod 26, so the function $f(x)$ is one-to-one. In other words, every letter of ciphertext can be obtained by exactly one letter of plaintext. Therefore `abe` is the only plaintext that encrypts to `ben`. □

(3) (a) Find all positive integers $0 < x < 21$ such that $x^2 \equiv 16 \pmod{21}$.
(b) Calculate $2^{29} \pmod{21}$. Your answer should be an integer between 0 and 20.

Solution:

Solution:

(a) Since $21 = 3 \cdot 7$ is a prime factorization, we want to solve

$$x^2 \equiv 16 \equiv 1 \pmod{3}$$
$$x^2 \equiv 16 \equiv 2 \pmod{7}.$$

If a nonzero number has a square root modulo a prime p, then it has exactly two square roots. Mod 3, the square roots of 1 are 1 and 2; mod 7, the square roots of 2 are 3 and 4. This gives a system of four congruences, each of which has a unique solution mod 21 by the Chinese remainder theorem:

$$\left\{ \begin{matrix} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{7} \end{matrix} \right\} \implies x \equiv 10 \pmod{21}$$

$$\left\{ \begin{matrix} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{7} \end{matrix} \right\} \implies x \equiv 4 \pmod{21}$$

$$\left\{ \begin{matrix} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{7} \end{matrix} \right\} \implies x \equiv 17 \pmod{21}$$

$$\left\{ \begin{matrix} x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{7} \end{matrix} \right\} \implies x \equiv 11 \pmod{21}$$

(b) Since $21 = 3 \cdot 7$, we have $\phi(21) = (3-1)(7-1) = 12$. Since $29 \equiv 5 \pmod{12}$, we have

$$2^{29} \equiv 2^5 \equiv 32 \equiv 11 \pmod{21}.$$

□

(4) 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.)

Solution:
Solution: Let $p = 991$ and $q = 607$. The decryption exponent d satisfies $de \equiv 1 \pmod{\phi(n)}$; that is, $\phi(n) \mid (de - 1)$. Since $\phi(n) = (p-1)(q-1)$, and since both $p - 1$ and $q - 1$ are even, $\phi(n)$ is divisible by 4. Thus $4 \mid (de - 1)$, so $de \equiv 1 \pmod 4$; hence

$$d \equiv e^{-1} \pmod 4.$$

(a) Since $e = 17 \equiv 1 \pmod 4$, we have

$$d \equiv e^{-1} \equiv 1^{-1} \equiv 1 \pmod 4.$$

(b) Since $e = 19 \equiv 3 \pmod 4$, we have

$$d \equiv e^{-1} \equiv 3^{-1} \equiv 3 \pmod 4.$$

□

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

Solution:
Solution: Since $60^2 \equiv 1 \pmod{3599}$, we have

$$60^2 - 1 \equiv 0 \pmod{3599} \implies (60-1)(60+1) \equiv 0 \pmod{3599} \implies 59 \cdot 61 \equiv 0 \pmod{3599}.$$

This shows that $3599 \mid 59 \cdot 61$. Since 59 and 61 are both prime, the only divisors of $59 \cdot 61$ are 1, 59, 61, and $59 \cdot 61$. Clearly $3599 \notin \{1, 59, 61\}$, so $3599 = 59 \cdot 61$. □

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

Solution:
Solution: We're given that $2^{10} \equiv 3 \pmod p$.
(a) Since

$$9 \equiv 3^2 \equiv \left(2^{10}\right)^2 \equiv 2^{20} \pmod p,$$

we have $L_2(9) = 20$.
(b) Since

$$6 \equiv 2 \cdot 3 \equiv 2 \cdot 2^{10} \equiv 2^{11} \pmod p,$$

we have $L_2(6) = 11$.

□

(7) 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) $(31, 4)$.

(8) *Solution:*
Solution: We just have to check, for each pair (m, k), whether $k^3 \equiv m \pmod{33}$. If so, then Alice signed the message; if not, she did not sign the message.
(a) $k^3 \equiv 3^3 \equiv 27 \equiv m \pmod{33}$, so Alice **did** sign the message.
(b) $k^3 \equiv 7^3 \equiv 13 \not\equiv m \pmod{33}$, so Alice **did not** sign the message.
(c) $k^3 \equiv 4^3 \equiv 31 \equiv m \pmod{33}$, so Alice **did** sign the message.

□

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

Solution:
Solution. (a) Using meet-in-the-middle by comparing $D_{K_1}(c)$ with $E_{K_2}(m)$, this should take about $2 \cdot 2^{56}$ steps. (b) Using meet-in-the-middle with $D_{K_1}(c)$ and $E_{K_2}(E_{K_3}(m))$, this will take about $2^{56} + 2^{56\cdot 2}$ steps (2^{112} is a fine approximation). (Note that there are three keys, so one might hope to get $2^{56\cdot 3}$, but you don't because of meet-in-the-middle attacks.) (c) Is exactly like (a), using $E_{K_2}(E_{K_2}(m))$ (only 2^{56} possibilities since it is K_2 twice) in place of $E_{K_2}(m)$, so $2 \cdot 2^{56}$ steps. For (d), there are no know meet-in-the-middle improvements so 2^{112} steps.

□

(9) 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.)

Solution:
Solution.

(a)This is the birthday problem with a search space of size 2^{224}, so one expects approximately $\sqrt{2^{224}} = 2^{112}$. (Technically, we say that calculating each hash takes about 224 steps so we might say $224 \cdot 2^{112}$, but that is not important.)

(b) In this case, you have to hit a specific value in your search space, so it should take about 2^{224} steps ($224 \cdot 2^{224}$ is a more precise estimate).

□

(10) 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 $h(m_1) = h(m_2)$.

Solution:
Solution. Since $\phi(7) = 6$ and $\phi(11) = 10$, we see that 3^{30} is congruent to 1 modulo 7 and 2^{30} is congruent to 1 modulo 7. Thus, $m_1 = 0$ and $m_2 = 31$ will work. □

(11) 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.]

Solution:

Solution. For (a), the numbers are clearly distinct since $m \geq 2$. To see this note that $2^m + 1$ and $2^m - 1$ are clearly distinct and that any other pair differ by at least $2^m - 2 > -0$. Now, clearly 1 and $2^{m+1} - 1$ clearly square to 1 modulo 2^{m+1}. For the other two, simply square and look at the remainder modulo 2^{m+1}, e.g.

$$(2^m + 1)^2 = 2^{2m} + 2 \cdot 2^m + 1 \equiv 1 \pmod{2^{m+1}}.$$

For (b), note that it follows immediately from the Chinese remainder and that furthermore 1, $4m-1$, $2m-1$ and $2m+1$ all work. For (c), observe that $(p-1)$ and $(q-1)$ are both even. For the last one, we note that $(p-1)(q-1)$ is at least 8. If it is divisible by 8, we get four square roots of one modulo 2^{m+1} giving us at least four modulo $(p-1)(q-1)$ by Chinese remainder. Otherwise, we apply (c).

□

(12) 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?

Solution:

This is the "baby-step, giant-step" method for solving for a discrete log. By constructing two lists and comparing the results the time used is converted from N to $\sqrt{N}$ steps plus a comparison search (which is $\log(N)$). Since $6^2 > N = 31$ it is the right choice for the length of the list.

In the list above there is a match when $i = 5$ in the first list and $i = 3$ in the second hence $3^5 \equiv 11 \cdot 3^{-3 \cdot 6} \pmod{31}$ or $3^{23} \equiv 11 \pmod{31}$

□

(13) Find the inverse of a polynomial in a finite field.
Let $GF = \{a_0 + a_1X + a_2X^2 + a_3X^3 + \cdots \mid \pmod{X^4 + X^2 + X + 1}\}$
$X^4 + X^2 + X + 1$ is an irreducible polynomial.
Find the inverse of $g = X + 1$ in this field.

Solution:

As with all finite modules we use the euclidean algorithm. $X^4+X^2+X+1 = (X+1)(X^3+X^2+1)$. Oops. It turns out $X^4 + X^2 + X + 1$ is not irreducible and $X + 1$ as one of its factors does not have an inverse. The irreducible polynomial should have been $X^4 + X^3 + X^2 + X + 1$ (there are other choices). In that case

$X^4 + X^3 + X^2 + X + 1 = (X^3 + X)(X + 1) + 1$ You don't even need to continue the euclidean algorithm we have

$1 = \gcd(X^4 + X^3 + X^2 + X + 1, X + 1) = (X + 1)(X^3 + X) + (X^4 + X^3 + X^2 + X + 1) \cdot 1$

and the inverse of $(X + 1)$ is $(X^3 + X)$

□

(14) 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.

Solution:

Suppose that $k = ord(7)$ is the smallest power where $7^k \equiv 1 \pmod{601}$. Then $k|600$ and if α is not primitive then $k < 600$, hence $k|300$ or $k|200$ or $k|120$. If k divides 300 for example then $7^{\equiv}1$ (mod 601) but this is not the case. Similarly for 200 and 120 hence $k = 600$ and 7 is a primitive root. □

(15)

(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.

Solution:

(a) $6^2 \equiv 3 \pmod{11}$ Hence $6^4 \equiv 9, \quad 6^5 \equiv 45 \equiv 1 \pmod{11}$.

(b) Given $2^x \equiv 6 \pmod{11}$ raise both sides to the $(p-1)/2 = (11-1)/2 = 5$ power. Since $2^{(p-1)/2} = -1$ we have $(-1)^x \equiv 6^5 \equiv 1 \pmod{11}$ so x must be even. □