HW 6 CMSC 456. DUE Oct 22
SOLUTIONS
NOTE- THE HW IS FIVE PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day and time of the first midterm? Read all of the slides on Public Key Crypto.

GOTO NEXT PAGE

2. (Read the slides on LWE-Diffie Helman) (WARNING- this problem continues onto the next page. Write the following programs. I highly suggest using python's numpy library to implement this easier.

   (a) $GENMATRIX(n, p)$: gen a rand $n \times n$ matrix of elements of $\{0, \ldots, p-1\}$. We view entries as elements of $\mathbb{Z}_p$.
   (See numpy.randint - it can generate random integer arrays. This can be done with one line)

   (b) $GENVEC(n, p)$: gen a rand n-vector of elements of $\{0, \ldots, p-1\}$. We view entries as elements of $\mathbb{Z}_p$.
   (See numpy.randint)

   (c) $GENERR(n, p)$: gen a rand n-vector of elements of $\{0, 1, p-1\}$. We view entries as elements of $\mathbb{Z}_p$.
   (See numpy.randint, you can use min = -1, max = 1 and then use % over the resulting array)

   (d) $GENDATA(n, p, N)$:

      i. $A := GENMATRIX(n, p)$
      ii. $\vec{y} := GENVEC(n, p)$
      iii. $\vec{e_y} := GENERR(n, p)$
      iv. $\vec{x} := GENVEC(n, p)$
      v. $\vec{e_x} := GENERR(n, p)$
      vi. $a = \vec{y}A\vec{x} + (\vec{y} \cdot \vec{e_x})$
      (numpy.mod(numpy.dot($\vec{y}, A$), p) can be used to preform a dot product over modulo p)
      vii. $b = \vec{y}A\vec{x} + (\vec{x} \cdot \vec{e_y})$
      viii. if $a \in \{0, \ldots, \lfloor p/4 \rfloor\} \cup \{\lfloor 3p/4 \rfloor, \ldots, p-1\}$ $\hat{a} = 0$, else $\hat{a} = 1$.
      ix. if $b \in \{0, \ldots, \lfloor p/4 \rfloor\} \cup \{\lfloor 3p/4 \rfloor, \ldots, p-1\}$, $\hat{b} = 0$, else $\hat{b} = 1$.
      x. the variable `agree` is YES if $\hat{a} = \hat{b}$ and NO otherwise.
      xi. Your code will output a tuple or an array of $[a, b, \hat{a}, \hat{b}, agree]$

GOTO NEXT PAGE

xii. Here is a sample of printing your output:
OUTPUT STARTS HERE
$n = 5$, $p = 17$, $N = 5$.

a	b	$\hat{a}$	$\hat{b}$	`agree`
3	2	0	0	YES
10	12	1	0	NO
7	9	1	1	YES
1	0	0	0	YES
5	6	0	0	YES

$\hat{a}$ and $\hat{b}$ agree 80% of the time.
END OF OUTPUT
*****Note that $N = 5$ and there are five lines.*****

GOTO NEXT PAGE

NOTE- For the above problems no points are given but submit anyway to help us grade the problems below which ARE for points.

NOTE- THIS IS STILL PROBLEM TWO:

(a) (10 points). Run program $GENDATA$ with the following inputs. Present the entire output. Using tabs (\t) to delineate variables makes the output more readable. You can pipe your code into a text file to make it easy to submit ex. `LWE.py >> output.txt`

i. $n = 4$, $p = 19$

ii. $n = 10$, $p = 23$

(b) Make a method to take $[n, p, N]$ as input and output the percent of agreement. Call this method $GENDATA2(n, p, N)$.

(c) Make a method to take a LIST of $[n, p, N]$ inputs and output a table of the n, p, N and percent of agreement. Call this method $GENDATA3(n, p, N)$. A sample output is:

n	p	N	`percent agree`
5	17	5	80
6	19	5	75
7	23	10	90

This can be generated by printing "n\tp\tN\tagree" If you follow this format for the entries of the table, your results should line up.

(d) (20 points) Run $GENDATA(n, p, N)$ on all $5 \leq n \leq 10$, all primes p where $11 \leq p \leq 23$, and $N = 10000$.

(e) (10 points) Note the highest and lowest percentages.

(f) (0 points) If you spot any trends in the data report them.

SOLUTION TO PROBLEM TWO

Omitted.

GOTO NEXT PAGE

3. (30 points). In class we tried to find m such that $m^2 \equiv 101 \pmod{1147}$. We noted that $1147 = 31 \times 37$ and that

   $m^2 \equiv 101 \equiv 8 \pmod{31}$ has solutions $m = \pm 15$ which is really $\{15, 16\}$

   $m^2 \equiv 101 \equiv 27 \pmod{37}$ has solutions $m = \pm 8$ which is really $\{8, 29\}$

   From the pair $(15, 8)$ we found that $m = 1007$ satisfies $m^2 \equiv 101 \pmod{1147}$.

   Find the other three square roots that same way. You must explain your procedure. You can use programs on line (tell us which ones) if you do Chinese Remainder Theorem, but you can't use a SQRT program.

   Clearly list all four square root in numeric order (to make life easier for the graders).

   ADVICE: Check your answer by squaring all four of them mod 1147 and seeing if you always get 101.

   SOLUTION TO PROBLEM THREE

   We used

   `https://www.dcode.fr/chinese-remainder`

   for our CRT calculations.

   $m \equiv 15 \pmod{31}$

   $m \equiv 29 \pmod{37}$

   CRT-calculator tells us that $m \equiv 325 \pmod{1147}$

   $m \equiv 16 \pmod{31}$

   $m \equiv 8 \pmod{37}$

   CRT-calculator tells us that $m \equiv 822 \pmod{1147}$

   $m \equiv 16 \pmod{31}$

   $m \equiv 29 \pmod{37}$

   CRT-calculator tells us that $m \equiv 140 \pmod{1147}$

   And the original one was 1007

   So the four square roots of 101 mod 1147 are

   $140, 325, 822, 1007$.

GOTO NEXT PAGE

4. (30 points). In this problem you will do the Blum-Williams variant of Rabin Encryption. Let $p = 3$, $q = 11$.

   (a) What is the Public Key?

   (b) List all m such that Bob can send m (encoded of course) to Alice. List the m's in numeric order (easy for the grader). And tell us how you got this list.

   (c) Alice gets 4 from Bob. What does Alice do to decode it? Give us all her steps and what the final answer is!

SOLUTION TO PROBLEM FOUR

a) The Public Key is $N = p \times q = 33$.

b) The only messages we can send are squares mod 33. So we need to find ALL of them to find the least five. Easy enough to do by hand, and since $a^2 = (-a)^2$ that cuts our work in half.

We first do them in the order of the squares then reorder

$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9, 4^2 = 16, 5^2 = 25,$

$6^2 = 36 \equiv 3$

$7^2 = 49 \equiv 16$

$8^2 = 64 \equiv 64 - 66 \equiv -2 \equiv 31$

$9^2 = 81 \equiv 81 - 66 \equiv 15$

$10^2 = 81 \equiv 100 - 99 \equiv 1$

$11^2 = 121 \equiv 121 - 99 \equiv 22$

$12^2 = 144 \equiv 144 - 132 \equiv 12$

$13^2 = 169 \equiv 169 - 132 \equiv 37 \equiv 4$

$14^2 = 196 \equiv 196 - 165 \equiv 31$

$15^2 = 225 \equiv 225 - 198 \equiv 27$

$16^2 = 225 \equiv 256 - 198 \equiv 58 \equiv 58 - 33 \equiv 25.$

Since $17^2 \equiv (33 - 17)^2 \equiv 16^2$ we can stop here.

We now put them in order.

$$0 < 1 < 3 < 4 < 9 < 12 < 15 < 16 < 22 < 25 < 27 < 31$$

3) Alice sees 4. She needs to find the sqrts of 4 mod 33. So she needs sqrt of 3 mod 3 and 11

$m^2 \equiv 4 \equiv 1 \pmod 3$ is $m = \pm 1$, so $m = 1, 2$.

$m^2 \equiv 4 \pmod{11}$ is $m = \pm 2$, so $m = 2, 9$.

Alice finds all four square roots based on these:

$m \equiv 1 \pmod 3$ and $m \equiv 2 \pmod{11}$. $m = 13$ works.

$m \equiv 1 \pmod 3$ and $m \equiv 9 \pmod{11}$. $m = 31$ works.

$m \equiv 2 \pmod 3$ and $m \equiv 2 \pmod{11}$. $m = 2$ works.

$m \equiv 2 \pmod 3$ and $m \equiv 9 \pmod{11}$. $m = 20$ works.

THEN Alice tests which of these are themselves squares. She finds out that only 31 is, so $m = 31$.