MATH 342—Quiz #5
June 14, 2006

No notes, books, or calculators allowed; put away all cell phones, pages, etc. and make sure that they won't beep. Show all your work and justify all of your responses fully, unless otherwise stated in the problem. You may write on the backs of pages if necessary. Do not remove the staple or any of the pages.

Name: Suggested Solutions **Student ID:** _____

1. For this problem, you only have to write the answers down—you don't have to prove anything.

(a) **[5 pts]** Explain the difference between public-key cryptography and private-key cryptography.

(b) **[5 pts]** We can program a computer to set up RSA private keys and to encrypt and decrypt messages using the RSA system; but our enemies can also program a computer to crack encrypted messages that we send to each other. Why then do we say that the RSA public-key cryptosystem is secure?

(a)- In private-key cryptography, the sender and the recipient agree beforehand on the cryptosystem to use, which requires secure meeting ahead of time. So, the only people that know the cryptosystem are the senders & recipient.

- In public-key cryptography, every recipient has his/her own copy of "public key". So anyone can encrypt and send messages to the recipient, but only the recipient holds the decryption key!

(b). The program we use to set up the RSA keys to encrypt/decrypt are all "fast" (polynomial) algorithms such as Euclidean algorithm and repeated squaring. But all known methods to crack RSA (brute force, factoring, discrete log) only have "slow" (non-polynomial or exponential) algorithm known. So, even with the help of computer, the enemy must still take a long long time if we pick n large enough, So cracking is possible theoretically but uselessly slow!

2. [**10 pts**] Of the two numbers 735 and 736, one of them (call it x) is relatively prime to 851, while the other one (call it y) isn't. Figure out which one is x and which one is y; find the multiplicative inverse of x modulo 851, and find $\gcd(y, 851)$.

Apply the Euclidean algorithm twice to both 735, 736 with 851.

(1) $\begin{bmatrix} 735 & 1 & 0 \\ 851 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 735 & 1 & 0 \\ 116 & -1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 39 & 7 & -6 \\ 116 & -1 & 1 \end{bmatrix}$

$\rightarrow \begin{bmatrix} 39 & 7 & -6 \\ 38 & -15 & 13 \end{bmatrix} \rightarrow \begin{bmatrix} (1) & (22) & -19 \\ 38 & -15 & 13 \end{bmatrix}$ (gcd, inverse)

$\therefore \gcd(735, 851) = 1 \Rightarrow x = 735$

$735^{-1} \equiv 22 \pmod{851}$.

(2) $\begin{bmatrix} 736 & 1 & 0 \\ 851 & 0 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 736 & 1 & 0 \\ 115 & -1 & 1 \end{bmatrix} \rightarrow \begin{bmatrix} 46 & 7 & -6 \\ 115 & -1 & 1 \end{bmatrix}$

$\rightarrow \begin{bmatrix} 46 & 7 & -6 \\ 23 & -15 & 13 \end{bmatrix} \rightarrow \begin{bmatrix} 0 & * & * \\ (23) & -15 & 13 \end{bmatrix}$ (gcd!)

$\therefore \gcd(736, 851) = 23 \Rightarrow y = 736$

3. [**10 pts**] You receive a message that was encrypted using the affine cipher $C \equiv 15P + 4 \pmod{26}$. If the ciphertext is DURA, decrypt the message (that is, find the original plaintext).

Translation table between letters and numbers

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

$C \equiv 15P+4 \pmod{26}$

$\therefore 15^{-1}(C-4) \equiv P \pmod{26}$. $\therefore$ We need to find $15^{-1} \pmod{26}$.

$$\begin{bmatrix} 15 & 1 & 0 \\ 26 & 0 & 1 \end{bmatrix} \to \begin{bmatrix} 15 & 1 & 0 \\ 11 & -1 & 1 \end{bmatrix} \to \begin{bmatrix} 4 & 2 & -1 \\ 11 & -1 & 1 \end{bmatrix} \to \begin{bmatrix} 4 & 2 & -1 \\ 3 & -5 & 3 \end{bmatrix}$$

$$\to \begin{bmatrix} 1 & 7 & -4 \\ 3 & -5 & 2 \end{bmatrix} \to \begin{bmatrix} 1 & 7 & -4 \\ 0 & * & * \end{bmatrix}.$$

$\therefore 7 \cdot 15 - 4 \cdot 26 = 1$

$\Rightarrow 15^{-1} \equiv 7 \pmod{26}$ $\therefore$

$\therefore P \equiv 7(C-4) \equiv 7C - 28 \equiv 7C - 2 \pmod{26}$.

	D	U	R	A
(C)	3	20	17	0
$(7C)$	21	10	15	0
$P=7C-2$	19	8	13	24.

T I N Y !

4.

(a) **[7 pts]** Using the RSA cryptosystem, with RSA modulus $n = 35$ and encryption exponent $e = 17$, encrypt the plaintext message WIRE into ciphertext. (Leave your ciphertext answer in numerical form, rather than English letters.)

(b) **[3 pts]** What is the decryption exponent d corresponding to $n = 35$ and $e = 17$?

Squares modulo 35

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
x^2	1	4	9	16	25	1	14	29	11	30	16	4	29	21	15	11	9
x	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
x^2	9	11	15	21	29	4	16	30	11	29	14	1	25	16	9	4	1

(a) Construct the following table in mod 35.

		W	I	R	E
	C	22	8	17	4
	C^2	29	29	9	16
C^{17}	C^4	1	1	11	11
	C^8	1	1	16	16
	C^{16}	1	1	11	11
$C^{16}\cdot C = C^{17}$		$1\cdot 22$	$1\cdot 8$	$11\cdot 17$	$11\cdot 4$

$\therefore$ 22, 8, 12, 9.

$\therefore 22^{17} \equiv 1\cdot 22 \equiv 22 \pmod{35}$.

$8^{17} \equiv 1\cdot 8 \equiv 8 \pmod{35}$

$17^{17} \equiv 17^{16}\cdot 17 \equiv 11\cdot 17 \equiv 187 \equiv 12 \pmod{35}$

$4^{17} \equiv 4^{16}\cdot 4 \equiv 11\cdot 4 \equiv 44 \equiv 9 \pmod{35}$

(b) $35 = 5\times 7 \Rightarrow \phi(35) = (5-1)\cdot(7-1) = 24$

$d \equiv e^{-1} \pmod{\phi(n)} \Rightarrow d = 17^{-1} \pmod{24}$

$$\begin{bmatrix} 17 & 1 & 0 \\ 24 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 17 & 1 & 0 \\ 7 & -1 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 3 & -2 \\ 7 & -1 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & * & * \\ 1 & (-7) & 5 \end{bmatrix}$$

inverse!

$\therefore d \equiv 17^{-1} \equiv -7 \pmod{24}$!

$\equiv 17$