7.5 An Application to Cryptography

Note Title 11/21/2005

1. Encrypt the message RETURN HOME using the Caeser cipher.

Using $A = 00$, $B = 01$, ..., $Z = 25$, and a space stays as a space,

R	E	T	U	R	N		H	O	M	E	
17	04	19	20	17	13		07	14	12	04	+3
20	7	22	23	20	16		10	17	15	07	

$\therefore$ UHWXUQ KRPH

2. If the Caeser cipher produced KDSSB ELUWKGDB, what is the plaintext message.

K	D	S	S	B		E	L	U	W	K	G	D	B	
10	03	18	18	01		04	11	20	22	10	06	03	01	−3
07	00	15	15	24		01	08	17	19	07	03	00	24	
H	A	P	P	Y		B	I	R	T	H	D	A	Y	

3. (a). A linear cipher is defined by $C \equiv aP + b \pmod{26}$, where a, b are integers, $\gcd(a, 26) = 1$. Show the decrypting sequence is: $P \equiv a'(C - b) \pmod{26}$ where a' satisfies: $aa' \equiv 1 \pmod{26}$.

Pf: Since $\gcd(a, 26) = 1$, Then by corollary to Th. 4.7 (p. 76), The linear congruence $ax \equiv 1 \pmod{26}$ has a unique solution. Let it be a'. $\therefore aa' \equiv 1 \pmod{26}$.

From $C \equiv aP + b \pmod{26}$,

$$C - b \equiv aP \pmod{26},$$

$$a'(C-b) \equiv a'aP \equiv P \pmod{26}$$

since $a'a \equiv 1 \pmod{26}$

$$\therefore P \equiv a'(C-b) \pmod{26}$$

(b) Using The linear cipher $C \equiv 5P + 11 \pmod{26}$, encrypt The message:

NUMBER THEORY IS EASY

Using $A = 00, B = 01, \ldots, Z = 25$,

N	U	M	B	E	R	T	H	E	O	R	Y	I	S	E	A	S	Y
13	20	12	1	4	17	19	7	4	14	17	24	8	18	4	0	18	24
76	111	71	16	31	96	106	46	31	81	96	131	51	101	31	11	101	131
24	7	19	16	5	18	2	20	5	3	18	1	25	23	5	11	23	1
Y	H	T	Q	F	S	C	U	F	D	S	B	Z	X	F	L	X	B

(c) Decrypt RZQTGU HOZTKGH DJ KTKMMTG, which was produced using the linear cipher $C \equiv 3P+7 \pmod{26}$.

From (a), $3x \equiv 1 \pmod{26}$

$$\therefore 27x \equiv 9 \pmod{26}$$
$$\therefore x \equiv 9 \pmod{26}$$

$\therefore$ let $a' = 9$ as in (a)

$$\therefore 9(C-7) \equiv 9(3P) = 27P \equiv P \pmod{26}$$

$$\therefore P \equiv 9C - 63 \equiv 9C + 15 \pmod{26}$$

RZQTGU $\quad C:$ 17, 25, 16, 19, 6, 20
$9(C-7)$: 90, 162, 81, 108, −9, 117
$9(C-7) \pmod{26}$: 12, 6, 3, 4, 17, 13
P: M G D E R N
(should have been RXQTGU ⇒ MODERN)

HOZTKGH $\quad C:$ 7, 14, 25, 19, 10, 6, 7
$9(C-7)$: 0, 63, 162, 108, 27, −9, 0
$9(C-7) \pmod{26}$: 0, 11, 6, 4, 1, 17, 0
P: A L G E B R A

AJ $\quad C: \ 3, 9$ $\quad$ (should have been FG ⇒ IS)

$9(C-7): \ -36, 18$

$9(C-7) \pmod{26}: \ 16, 18$

$P: \ Q \ S$

KTKMMTG $\quad C: \ 10, 19, 10, 12, 12, 19, 6$

$9(C-7): \ 27, 108, 27, 45, 45, 108, -9$

$9(C-7) \pmod{26}: \ 1, 4, 1, 19, 19, 4, 17$

$P: \ B \ E \ B \ T \ T \ E \ R$

(should have been KTMMTG)

4. In a lengthy ciphertext message, sent using a linear cipher $C \equiv aP + b \pmod{26}$, the most frequently occurring letter is Q and the second most frequent is J.

(a) Break the cipher by determining the values of a and b.

$Q \Rightarrow 16, \ J \Rightarrow 9$

$$\therefore \ 16 \equiv aP_1 + b \pmod{26}$$
$$9 \equiv aP_2 + b \pmod{26}$$

As the message is lengthy, P_1 likely is E and P_2 likely is T.

$\therefore P_1 = E \Rightarrow 4$
$\quad P_2 = T \Rightarrow 19$

$\therefore 16 \equiv 4a + b \pmod{26}$
$\quad 9 \equiv 19a + b \pmod{26}$

$\therefore 7 \equiv -15a \pmod{26}$
$\quad 30a \equiv -14,\ 30a - 26a \equiv -14,\ 4a \equiv -14,\ 4a \equiv 12,$
$\quad a \equiv 3 \pmod{26}$
$\therefore 4a \equiv 12,\ \therefore b \equiv 4 \pmod{26}$

$\therefore a = 3,\ b = 4$

(b) Using (a), $C \equiv 3P + 4 \pmod{26}$,
$\quad C - 4 \equiv 3P \pmod{26}$
$\quad 9(C-4) \equiv 27P \equiv P \pmod{26}$
$\therefore P = 9(C-4) \pmod{26}$

WCPQ

C:	22, 2, 15, 16
$9(C-4)$:	162, −18, 99, 108
$9(C-4) \pmod{26}$:	6, 8, 21, 4
P:	G I V E

$$\begin{array}{rl}
JZQO \qquad C: & 9,\ 25,\ 16,\ 14 \\
9(C-4): & 45,\ 189,\ 108,\ 90 \\
9(C-4) \pmod{26}: & 19,\ 7,\ 4,\ 12 \\
P: & T\ H\ E\ M
\end{array}$$

$$\begin{array}{rl}
MX \qquad C: & 12,\ 23 \\
9(C-4): & 72,\ 171 \\
9(C-4) \pmod{26}: & 20,\ 15 \\
P: & U\ P
\end{array}$$

5. (a) Encipher the message HAVE A NICE TRIP using a Vigenère cipher with the keyword MATH.

MATH $\Rightarrow$ 12 00 19 07

$$\begin{array}{rcccccccccccccc}
 & H & A & V & E & A & N & I & C & E & T & R & I & P & \\
 & 7 & 0 & 21 & 4 & 0 & 13 & 8 & 2 & 4 & 19 & 17 & 8 & 15 & \\
+ & 12 & 0 & 19 & 7 & 12 & 0 & 19 & 7 & 12 & 0 & 19 & 7 & 12 & \\
 & 19 & 0 & 40 & 11 & 12 & 13 & 27 & 9 & 16 & 19 & 36 & 15 & 27 & \\
 & 19 & 0 & 14 & 11 & 12 & 13 & 1 & 9 & 16 & 19 & 10 & 15 & 1 & \pmod{26}
\end{array}$$

TAOL M NBJQ TKPB

(b) The ciphertext BS FMX KFSGR JAPWL is

Known to have resulted from a Vigenére cipher whose Keyword is YES. Obtain the deciphering congruences and read the message.

YES = 24 4 18. Subtract YES (mod 26) from ciphertext to get plaintext.

B	S	F	M	X	K	F	S	G	R	J	A	P	W	L	
1	18	5	12	23	10	5	18	6	17	9	0	15	22	11	
24	4	18	24	4	18	24	4	18	24	4	18	24	4	18	YES
															−YES
3	14	13	14	19	18	7	14	14	19	5	8	17	18	19	(mod 26)
D	O	N	O	T	S	H	O	O	T	F	I	R	S	T	

6. (a). Use the Hill cipher $C_1 \equiv 5P_1 + 2P_2 \pmod{26}$
$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$

to encipher GIVE THEM TIME

Note $\gcd(5\cdot4-3\cdot2, 26) = \gcd(14, 26) = 2$, so you can encipher, but not decipher.

G	I	V	E	T	H	E	M	T	I	M	E
6	8	21	4	19	7	4	12	19	8	12	4

Break up text in blocks of 2 letters.

GI: $C_1 \equiv 5(6) + 2(8) = 40 \equiv 14 \pmod{26} \Rightarrow O$
$C_2 \equiv 3(6) + 4(8) = 50 \equiv 24 \pmod{26} \Rightarrow Y$

VE: $C_1 \equiv 5(21) + 2(4) = 113 \equiv 9 \Rightarrow J$
$C_2 \equiv 3(21) + 4(4) = 79 \equiv 1 \Rightarrow B$

TH: $C_1 \equiv 5(19) + 2(7) = 109 \equiv 5 \Rightarrow F$
$C_2 \equiv 3(19) + 4(7) = 85 \equiv 7 \Rightarrow H$

EM: $C_1 \equiv 5(4) + 2(12) = 44 \equiv 18 \Rightarrow S$
$C_2 \equiv 3(4) + 4(12) = 60 \equiv 8 \Rightarrow I$

TI: $C_1 \equiv 5(19) + 2(8) = 111 \equiv 7 \Rightarrow H$
$C_2 \equiv 3(19) + 4(8) = 89 \equiv 11 \Rightarrow L$

ME: $C_1 \equiv 5(12) + 2(4) = 68 \equiv 16 \Rightarrow Q$
$C_2 \equiv 3(12) + 4(4) = 52 \equiv 0 \Rightarrow A$

$\therefore$ OYJB FHSI HLQA

(b). The ciphertext ALXWU VADCOJO has been enciphered using $C_1 \equiv 4P_1 + 11P_2 \pmod{26}$
$C_2 \equiv 3P_1 + 8P_2 \pmod{26}$

Derive the plaintext.

Note $\gcd(4\cdot 8-3\cdot 11, 26) = \gcd(-1, 26) = 1$

$$\begin{aligned} 3C_1 &\equiv 12P_1 + 33P_2 \pmod{26} \\ 4C_2 &\equiv 12P_1 + 32P_2 \pmod{26} \end{aligned}$$

$$\begin{aligned} 8C_1 &\equiv 32P_1 + 88P_2 \\ 11C_2 &\equiv 33P_1 + 88P_2 \end{aligned}$$

$3C_1 - 4C_2 \equiv P_2 \pmod{26}$ $\qquad$ $11C_2 - 8C_1 \equiv P_1 \pmod{26}$

A	L	X	W	U	V	A	D	C	O	J	O
0	11	23	22	20	21	0	3	2	14	9	14

AL: $P_1 \equiv -8(0) + 11(11) = 121 \equiv 17 \Rightarrow R$
$P_2 = 3(0) - 4(11) = -44 \equiv 8 \Rightarrow I$

XW: $P_1 \equiv -8(23) + 11(22) = 58 \equiv 6 \Rightarrow G$
$P_2 \equiv 3(23) - 4(22) = -19 \equiv 7 \Rightarrow H$

UV: $P_1 \equiv -8(20) + 11(21) = 71 \equiv 19 \Rightarrow T$
$P_2 \equiv 3(20) - 4(21) = -24 \equiv 2 \Rightarrow C$

AD: $P_1 \equiv -8(0) + 11(3) = 33 \equiv 7 \Rightarrow H$
$P_2 \equiv 3(0) - 4(3) = -12 \equiv 14 \Rightarrow O$

CO: $P_1 \equiv -8(2) + 11(14) = 138 \equiv 8 \Rightarrow I$
$P_2 \equiv 3(2) - 4(14) = -50 \equiv 2$ C

JO: $P_1 \equiv -8(9) + 11(14) = 82 \equiv 4 \Rightarrow E$
$P_2 \equiv 3(9) - 4(14) = -29 \equiv 23 \Rightarrow X$

$\therefore$ RIGHT CHOICEX

(Last two enciphered letters should have been GA to make plaintext CHOICES).

7. A long string of ciphertext resulting from a Hill cipher

$$C_1 \equiv aP_1 + bP_2 \pmod{26}$$
$$C_2 \equiv cP_1 + dP_2 \pmod{26}$$

revealed that the most frequently occurring two-letter blocks were HO and PP, in that order.

(a) Find the values of a, b, c, d

Using the hint that the most common 2-letter blocks in English are TH and then HE, we have:

$$H \equiv a(T) + b(H) \pmod{26} \quad [1]$$
$$O \equiv c(T) + d(H) \pmod{26} \quad [2]$$

and:

$$P \equiv a(H) + b(E) \pmod{26} \quad [3]$$
$$P \equiv c(H) + d(E) \pmod{26} \quad [4]$$

Or, using $00 \Rightarrow A, \ldots, 25 \Rightarrow Z$

$$7 \equiv 19a + 7b \pmod{26} \quad [1]$$
$$14 \equiv 19c + 7d \pmod{26} \quad [2]$$

$$15 \equiv 7a + 4b \pmod{26} \quad [3]$$
$$15 \equiv 7c + 4d \pmod{26} \quad [4]$$

From [1] and [3], $7 \equiv 19a + 7b \pmod{26}$
$15 \equiv 7a + 4b \pmod{26}$

Note that $\gcd(19\cdot 4 - 7\cdot 7, 26) = \gcd(27, 26) = 1$

$\therefore\ 28 \equiv 76a + 28b$
$105 \equiv 49a + 28b$

$-77 \equiv 27a \pmod{26}$
$-77 + 3\cdot 26 \equiv 27a - 26a$
$1 \equiv a \pmod{26}$

$\therefore\ 7 \equiv 19 + 7b$
$-12 \equiv 7b$
$14 \equiv 7b$
$2 \equiv b \pmod{26}$
as $\gcd(7, 26) = 1$

$\therefore\ a = 1,\ b = 2$

From [2], [4], $14 \equiv 19c + 7d \pmod{26}$
$15 \equiv 7c + 4d \pmod{26}$

and $\gcd(4\cdot 19 - 7\cdot 7, 26) = \gcd(27, 26) = 1$

$\therefore\ 56 \equiv 76c + 28d$

$\underline{105 \equiv 49c + 28d}$

$-49 \equiv 27c \pmod{26}$

$\therefore\ 3 \equiv c \pmod{26}$

$14 \equiv 57 + 7d,\ -43 \equiv 7d,$
$9 \equiv 7d,\ 99 \equiv 77d,$
$21 \equiv -d,\ d \equiv -21,$
$d \equiv 5$

$\therefore\ \underline{\underline{c = 3,\ d = 5}}$

$\therefore\ C_1 \equiv P_1 + 2P_2 \pmod{26}$
$C_2 \equiv 3P_1 + 5P_2 \pmod{26}$

(b) What is the plain text for the intercepted message: PPIH HOG RAPVT

From (a) $3C_1 \equiv 3P_1 + 6P_2$
$\underline{C_2 \equiv 3P_1 + 5P_2}$
$3C_1 - C_2 \equiv P_2$

$5C_1 \equiv 5P_1 + 10P_2$
$\underline{2C_2 \equiv 6P_1 + 10P_2}$
$2C_2 - 5C_1 \equiv P_1$

$\therefore\ P_1 \equiv -5C_1 + 2C_2 \pmod{26}$
$P_2 \equiv 3C_1 - C_2 \pmod{26}$

P	P	I	H	H	O	G	R	A	P	V	T
15	15	8	7	7	14	6	17	0	15	21	19

PP: HE

IH: 8, 7 $\quad p_1 \equiv -5(8) + 2(7) = -26 \equiv 0 \Rightarrow A$

$\quad\quad\quad\quad p_2 \equiv 3(8) - 7 = 17 \Rightarrow R$

HO : TH

GR : 6, 17 $\quad p_1 \equiv -5(6) + 2(17) = 4 \Rightarrow E$

$\quad\quad\quad\quad p_2 \equiv 3(6) - 17 = 1 \Rightarrow B$

AP: 0, 15 $\quad p_1 \equiv -5(0) + 2(15) = 30 \equiv 4 \Rightarrow E$

$\quad\quad\quad\quad p_2 \equiv 3(0) - 15 = -15 \equiv 11 \Rightarrow L$

VT: 21, 19 $\quad p_1 \equiv -5(21) + 2(19) = -67 \equiv 11 \Rightarrow L$

$\quad\quad\quad\quad p_2 \equiv 3(21) - 19 = 44 \equiv 18 \Rightarrow S$

$\therefore$ HEAR THE BELLS

8. If $n = pq = 274279$, and $\phi(n) = 272376$, find the primes p and q.

Use the hint. Note, since $n = pq$, $\phi(n) = (p-1)(q-1)$

$\therefore n - \phi(n) = pq - (p-1)(q-1)$

$= pq - [pq - p - q + 1] = p + q - 1$

$\therefore p+q = n - \phi(n) + 1$

Also, $p-q = [(p-q)^2]^{\frac{1}{2}} = [p^2 - 2pq + q^2]^{\frac{1}{2}}$

$= [p^2 + 2pq + q^2 - 4pq]^{\frac{1}{2}}$

$= [(p+q)^2 - 4n]^{\frac{1}{2}}$

$\therefore p+q = n - \phi(n) + 1 = 274279 - 272376 + 1 = 1904$

$p-q = [(p+q)^2 - 4n]^{\frac{1}{2}}$

$\therefore 2p = n - \phi(n) + 1 + [(n - \phi(n) + 1)^2 - 4n]^{\frac{1}{2}}$

$= 1904 + [1904^2 - 4(274279)]^{\frac{1}{2}}$

$= 1904 + [2528100]^{\frac{1}{2}} = 1904 + 1590$

$= 3494$

$\therefore \underline{p = 1747}, \underline{q = 157}$

9. When the RSA algorithm is based on the Key $(n, k) = (3233, 37)$ what is the

recovery exponent for the cryptosystem?

The recovery exponent is integer j satisfying

$Kj \equiv 1 \pmod{\phi(n)}$, or

$37j \equiv 1 \pmod{\phi(3233)}$

The prime factorization of 3233:

$\sqrt{3233} = 56.8$, so $p \leq 56$. $3233 = 53 \cdot 61$

$\therefore \phi(n) = 52(60) = 3120$

$\therefore 37j \equiv 1 \pmod{3120}$

Now $\gcd(37, 3120) = 1$ since

$3120 = 10(312) = 5 \cdot 2 \cdot 2 \cdot 156 = 2^2 5 \cdot (3 \cdot 2 \cdot 26)$
$= 2^4 \cdot 3 \cdot 5 \cdot 13$

$\therefore$ By prob. # 8(a), sec. 7.3, the solution

is $j \equiv 37^{\phi(3120)-1} \pmod{3120}$

$\phi(3120) = (2^4 - 2^3) \cdot (2)(4)(12) = 768$

$\therefore\ j \equiv 37^{767} \pmod{3120}$

Note that since $3120 = 2^4 \cdot 3 \cdot 5 \cdot 13$, gcd of 37 and any of these factors is 1.

$\therefore\ \phi(13) = 12$, so by Euler's Th., $37^{12} \equiv 1 \pmod{13}$

$\therefore\ 37^{12} \equiv 1 \pmod{3120}$

$767 = 12 \cdot 63 + 11$

$\therefore\ 37^{767} = (37^{12})^{63} \cdot 37^{11} \equiv 1^{63} \cdot 37^{11} \equiv 37^{11} \pmod{3120}$

$\therefore\ j \equiv 37^{11} \pmod{3120}$

$37^3 = 50653 = 3120 \cdot 16 + 733$

$\therefore\ 37^3 \equiv 733 \pmod{3120}$

$\therefore\ 37^6 \equiv 733^2 = 537289 = 172 \cdot 3120 + 649$

$\therefore\ 37^6 \equiv 649 \pmod{3120}$

$\therefore\ 37^9 \equiv 733 \cdot 649 = 475717 = 152 \cdot 3120 + 1477$

$\therefore\ 37^9 \equiv 1477 \pmod{3120}$

$37^2 = 1369$

$\therefore\ 37^{11} \equiv 1477 \cdot 1369 = 2022013 = 648 \cdot 3120 + 253$

$\therefore\ 37^{11} \equiv 253 \pmod{3120}$

$\therefore\ \underline{j \equiv 253 \pmod{3120}}$

10. Encrypt the plaintext message GOLD MEDAL using the RSA algorithm with key $(n,k)=(2419,3)$.

Using 99 for the space between words,

G	O	L	D		M	E	D	A	L
06	14	11	03	99	12	04	03	00	11

$\therefore m' = 6141103991204030011$

With $n=2419$, m' is broken into blocks of 3 digits, starting from the right.

$\therefore$ 006 141 103 991 204 030 011

Now convert each block using:

$$M_i^{\,k} \equiv r \pmod{n}, \text{ or } M_i^{\,3} \equiv r \pmod{2419}$$

006: $6^3 \equiv 216 \pmod{2419}$

141: $141^3 = 2803221 = 1158 \cdot 2419 + 2019$

$\therefore 141^3 \equiv 2019 \pmod{2419}$

103: $103^3 = 1092727 = 451 \cdot 2419 + 1758$

$\therefore 103^3 \equiv 1758 \pmod{2419}$

991: $991^3 = 973242271 = 402332 \cdot 2419 + 1163$

$\therefore 991^3 \equiv 1163 \pmod{2419}$

204: $204^3 = 8489664 = 3509 \cdot 2419 + 1393$

$\therefore 204^3 \equiv 1393 \pmod{2419}$

030: $30^3 = 27000 = 11 \cdot 2419 + 391$

$\therefore 30^3 \equiv 391 \pmod{2419}$

011: $11^3 = 1331$

$\therefore 11^3 \equiv 1331 \pmod{2419}$

$\therefore$ Ciphertext is:

0216 2019 1758 1163 1393 0391 1331

To check, note $2419 = 41 \cdot 59$,

$\therefore \phi(2419) = 40 \cdot 58 = 2320$

$\therefore kj \equiv 1 \pmod{\phi(n)} \Rightarrow 3j \equiv 1 \pmod{2320}$

$\therefore 773 \cdot 3j \equiv 773,\ 2319j \equiv 773,\ -j \equiv 773,$

$j \equiv -773 \equiv 2320 - 773 = 1547$

$\therefore j \equiv 1547 \pmod{2320}$

$\therefore 216^{1547} = (6^3)^{1547} = 6^{4641} = 6^{2 \cdot 2320 + 1}$

$\equiv 6 \pmod{2320}$

$\therefore$ First code is 006

So can reconstitue m', which is then broken into 2-digit numbers (starting from right) to get the letters.

11. The ciphertext message produced by the RSA algorithm with key $(n,k) = (1643, 223)$ is:

0833 0823 1130 0055 0329 1099

Determine the original plaintext message.

Note: to get $j = ?$ for recovery exponent, $\underline{k = 223}$, not 233. Both are prime, but assume a typo in book.

On the receiving side, $1643 = 31 \cdot 53$

$\therefore \phi(n) = 30 \cdot 52 = 1560$

Recovery exponent: $kj \equiv 1 \pmod{\phi(n)}$, or

$223j \equiv 1 \pmod{1560}$

From 8.(a), sec. 7.3, solution is $j \equiv 223^{\phi(1560)-1}$

$1560 = 2^3 \cdot 3 \cdot 5 \cdot 13$

$\therefore \phi(1560) = 4 \cdot 2 \cdot 4 \cdot 12 = 384$

$\therefore j \equiv 223^{383} \pmod{1560}$

Since $\gcd(13, 223) = 1$, $223^{12} \equiv 1 \pmod{13}$

$\therefore 223^{12} \equiv 1 \pmod{1560}$

$383 = 31 \cdot 12 + 11$

$\therefore 223^{383} = (223^{12})^{31} \cdot 223^{11} \equiv 223^{11} \pmod{1560}$

$\therefore j \equiv 223^{11} \pmod{1560}$

$223^2 = 32 \cdot 1560 - 191$, $\therefore 223^2 \equiv -191 \pmod{1560}$

$223^4 = (-191)^2 = 23 \cdot 1560 + 601$

$\therefore 223^8 \equiv 601^2 = 231 \cdot 1560 + 841$

$\therefore 223^8 \equiv 841$, $\therefore 223^{10} \equiv (841)(-191) = -160631$

$= -103 \cdot 1560 + 49$

$\therefore 223^{10} \equiv 49 \pmod{1560}$

$\therefore 223^{11} \equiv 49 \cdot 223 = 10927 = 7 \cdot 1560 + 7$

$\therefore j \equiv 223^{11} \equiv 7 \pmod{1560}$

$\therefore$ recovery exponent is $j = 7$

$\therefore$ modulo 1643

0833: 833^7: $833^2 = 693889 = 422 \cdot 1643 + 543$

$833^4 \equiv 543^2 = 294849 = 179 \cdot 1643 + 752$

$833^6 \equiv 543 \cdot 752 = 248 \cdot 1643 + 872$

$\therefore 833^7 \equiv 872 \cdot 833 = 442 \cdot 1643 + 170$

$\therefore 833^7 \equiv \underline{170} \pmod{1643}$

0823: 823^7: $823^2 \equiv 413$ (using a calculator)

$823^4 \equiv 1340$

$823^6 \equiv 1372$

$823^7 \equiv \underline{415}$

1130 : 1130^7: $1130^2 \equiv 289$

$1130^4 \equiv 1371$

$1130^6 \equiv 256$

$1130^7 \equiv \underline{112}$

0055: 55^7 : $55^3 \equiv 432$

$55^6 \equiv 965$

$55^7 \equiv \underline{499}$

0329: 329^7: $329^3 \equiv 807$

$329^6 \equiv 1149$

$329^7 \equiv \underline{131}$

1099 : 1099^7 : $1099^3 \equiv 171$

$1099^6 \equiv 1310$

$1099^7 \equiv \underline{422}$

$\therefore M = 170415112499131422$

17 04 15 11 24 99 13 14 22

$\therefore$ R E P L Y ␣ N O W

12. Decrypt the ciphertext

1369 1436 0119 0385 0434 1580 0690

that was encrypted using the RSA algorithm with key $(n,k) = (2419, 211)$.

$n = 2419 = 41 \cdot 59$. $\therefore \phi(n) = 40 \cdot 58 = 2320 = 2^4 \cdot 5 \cdot 29$

$\therefore 211j \equiv 1 \pmod{2320}$ $\quad \gcd(2320, 211) = 1$

Using prob. 8.a., Sec. 2.3,

$\phi(2320) = 8 \cdot 4 \cdot 28 = 896$, $\therefore j \equiv 211^{895} \pmod{2320}$

$\gcd(29, 211) = 1$, $\therefore 211^{28} \equiv 1 \pmod{29}$ by Fermat's Theorem

$895 = 31 \cdot 28 + 27$ $\therefore 211^{895} = (211^{28})^{31} \cdot 211^{27}$

$\therefore j \equiv 211^{895} \equiv 211^{27} \pmod{2320}$

$211^3 \equiv 251 \pmod{2320}$ [calculator]

$211^6 \equiv 251^2 \equiv 361 \pmod{2320}$

$211^{12} \equiv 361^2 \equiv 401$

$211^{24} \equiv 401^2 \equiv 721$

$\therefore 21^{27} \equiv 251 \cdot 721 \equiv 11 \pmod{2320}$

$\therefore$ recovery exponent $= 11$

$\therefore$ modulo 2419,

1369 :
$1369^2 \equiv 1855$
$1369^4 \equiv 1855^2 \equiv 1207$
$1369^8 \equiv 1207^2 \equiv 611$
$1369^{10} \equiv 611 \cdot 1855 \equiv 1313$
$1369^{11} \equiv 1313 \cdot 1369 \equiv \underline{180}$

1436 :
$1436^2 \equiv 1108$
$1436^4 \equiv 1231$
$1436^8 \equiv 1067$
$1436^{10} \equiv 1764$
$1436^{11} \equiv 1764 \cdot 1436 \equiv \underline{411}$

0119 :
$119^3 \equiv 1535$
$119^6 \equiv 119$
$119^9 \equiv 1535 \cdot 119 \equiv 1240$
$119^{11} \equiv 1240 \cdot 119^2 \equiv \underline{119}$

0385 :
$385^2 \equiv 666$
$385^4 \equiv 879$
$385^8 \equiv 980$
$385^{10} \equiv 1969$
$385^{11} \equiv \underline{918}$

0434 : $434^2 \equiv 2093$

$434^4 \equiv 2259$

$434^8 \equiv 1410$

$434^{10} \equiv 2369$

$434^{11} \equiv \underline{71} \Rightarrow 071$

1580 : $1580^2 \equiv 2411$

$1580^4 \equiv 64$

$1580^8 \equiv 1677$

$1580^{10} \equiv 1098$

$1580^{11} \equiv \underline{417}$

0690 : $690^2 \equiv 1976$

$690^4 \equiv 310$

$690^8 \equiv 1759$

$690^{10} \equiv 2100$

$690^{11} \equiv \underline{19} \Rightarrow$

Since $n = 2419$, plaintext should have been broken up into 3-digit blocks.

$\therefore$ 180411119918071417 19

18 04 11 11 99 18 07 14 17 19

S E L L ␣ S H O R T

So, wasn't enciphered properly, since only 10

2-digits codes (20 numbers).
Should have been (multiple of 3):

01804111199180714 1719

and $\therefore$ 018, 041, 111, 991, 807, 141, 719
i.e., for consistency, how do you know to precede 71 above so it's 071, but 19 isn't translated to 019.
The only way to know is always precede a 2-digit decrypted number with 0 until get to end: if need it, add the 0, if don't, don't do it: confusing.

i.e., when decrypting, must know size of block of plaintext that was enciphered. Should then use same block size when deciphering.

13. Obtain all solutions of the Knapsack problem

$$21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5 + 11x_6$$

Let $x_6 = 1$: $x_5 \neq 1$ since no possible "1"

$\therefore x_5 = 0$

$\therefore 10 = 2x_1 + 3x_2 + 5x_3 + 7x_4$

$x_4 = 1$: $x_1 = 0, x_2 = 1, x_3 = 0$

$x_4 = 0$: $x_1 = 1, x_2 = 1, x_3 = 1$

$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{0, 1, 0, 1, 0, 1\}$
or $\{1, 1, 1, 0, 0, 1\}$

Let $x_6 = 0$: $21 = 2x_1 + 3x_2 + 5x_3 + 7x_4 + 9x_5$

Let $x_5 = 1$: $12 = 2x_1 + 3x_2 + 5x_3 + 7x_4$

$\therefore x_1 = 0, x_2 = 0, x_3 = 1, x_4 = 1$

$x_1 = 1, x_2 = 1, x_3 = 0, x_4 = 1$

no solution if $x_4 = 0$

$\therefore \{0, 0, 1, 1, 1, 0\}$,
$\{1, 1, 0, 1, 1, 0\}$

Let $x_5 = 0$: $21 = 2x_1 + 3x_2 + 5x_3 + 7x_4$
No solution even if all $= 1$.

$\therefore$ All solutions:

x_1	x_2	x_3	x_4	x_5	x_6
0	1	0	1	0	1
1	1	1	0	0	1
0	0	1	1	1	0
1	1	0	1	1	0

14. Determine which of the sequences below is superincreasing:

(a) 3, 13, 20, 37, 81

$3 < 13$, $3+13 < 20$, $3+13+20 < 37$, $3+13+20+37 < 81$

$\therefore$ yes, it is superincreasing

(b) 5, 13, 25, 42, 90

No, since $5 + 13 + 25 = 43 > 42$

(c) 7, 27, 47, 97, 197, 397

$7+27 < 47$, $2(47) < 97$, $2(97) < 197$, $2(197) < 397$

$\therefore$ yes, it's superincreasing

15. Find the unique solution of each of the following superincreasing Knapsack problems:

(a) $118 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5 + 99x_6$

Since $4+5+10+20+41 = 80 < 118$, Then $x_6 \neq 0$

$\therefore x_6 = 1$, $\therefore 19 = 4x_1 + 5x_2 + 10x_3 + 20x_4 + 41x_5$

$\therefore x_5 = 0$ $(41 > 19)$

$x_4 = 0$ $(20 > 19)$

$\therefore x_1 = x_2 = x_3 = 1$

$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{1, 1, 1, 0, 0, 1\}$

(b) $51 = 3x_1 + 5x_2 + 9x_3 + 18x_4 + 37x_5$

Since $3+5+9+18 = 35 < 51$, x_5 must be 1.

$\therefore x_5 = 1$, $14 = 3x_1 + 5x_2 + 9x_3 + 18x_4$

$\therefore x_4 = 0$ $(18 > 14)$

If $x_3 = 1$, Then $x_2 = 1$, $x_1 = 0$

$x_3 = 0$, no solution.

$\therefore \{x_1, x_2, x_3, x_4, x_5\} = \{0, 1, 1, 0, 1\}$

(c) $54 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5 + 40x_6$

Since $1+2+5+9+18 = 35 < 54$, x_6 must be 1

$\therefore x_6 = 1$: $14 = x_1 + 2x_2 + 5x_3 + 9x_4 + 18x_5$

$\therefore x_5 = 0$ $(18 > 14)$

Let $x_4 = 1$. $\therefore x_1 = 0, x_2 = 0, x_3 = 1$

$x_4 = 0$: no solution

$\therefore \{x_1, x_2, x_3, x_4, x_5, x_6\} = \{0, 0, 1, 1, 0, 1\}$

16. Consider a sequence of positive integers $a_1, \ldots, a_n$, where $a_{i+1} > 2a_i$, for $i = 1, \ldots, n-1$. Show That the sequence is superincreasing.

Pf: By induction, for $n=2$, $a_2 > 2a_1$, so $a_2 > a_1$.

For $n = 3$, $a_3 > 2a_2 = a_2 + a_2 > a_2 + (2a_1)$
$$> a_2 + a_1$$

$\therefore$ Assume sequence is superincreasing for $K > 3$ (i.e., $a_K > a_1 + a_2 + \dots + a_{K-1}$)

$\therefore a_{K+1} > 2a_K$, by definition

$\therefore a_{K+1} > a_K + a_K$

$$> a_K + (a_1 + a_2 + \dots + a_{K-1})$$

$\therefore a_{K+1} > a_1 + a_2 + \dots + a_{K-1} + a_K$

$\therefore$ Superincreasing for all n

17. A user of the Knapsack cryptosystem has the sequence 49, 32, 30, 43 as a listed encryption key. If the user's private key involves the modulus $m = 50$ and multiplier $a = 33$, determine the secret superincreasing sequence.

Let a_1, a_2, a_3, a_4 be the superincreasing sequence

Note that $\gcd(33, 50) = 1$, so $b_i \equiv 33a_i \pmod{50}$

has a unique solution for a_i, given b_i (by corollary to Th. 4.7, sec. 4.4, on p. 76).

$\therefore$ $33a_1 \equiv 49 \pmod{50}$
$99a_1 \equiv 3(49) - 150$
$-a_1 \equiv -3$
$a_1 \equiv 3$

$33a_2 \equiv 32 \pmod{50}$
$99a_2 \equiv 96 - 100$
$-a_2 \equiv -4$
$a_2 \equiv 4$

$33a_3 \equiv 30 \pmod{50}$
$99a_3 \equiv 90 - 100$
$-a_3 \equiv -10$
$a_3 \equiv 10$

$33a_4 \equiv 43 \pmod{50}$
$99a_4 \equiv 3(43) - 150$
$-a_4 \equiv -21$
$a_4 \equiv 21$

$\therefore$ $a_1, a_2, a_3, a_4 = 3, 4, 10, 21$

18. The ciphertext message produced by The Knapsack cryptosystem employing the superincreasing sequence 1, 3, 5, 11, 35, modulus $m = 73$ and multiplier $a = 5$ is: 55, 15, 124, 109, 25, 34. Obtain The plaintext message.

(1) First find The unique solution to:
(multiplier) $x \equiv 1$ (mod modulus), or
$5x \equiv 1 \pmod{73}$ (note $\gcd(5, 73) = 1$).
$29(5x) \equiv 29$, $145x - 146x \equiv 29$,
$x \equiv -29 + 73$, $\underline{x \equiv 44}$

(2) Now convert ciphertext using
$s' \equiv 44s \pmod{73}$

55: $s' \equiv 44(55) \pmod{73}$ (using calculator)
$s' \equiv \underline{11}$

15: $s' \equiv 44(15) \pmod{73}$
$s' \equiv \underline{3}$

124: $s' \equiv 44(124) \pmod{73}$
$s' \equiv \underline{54}$

109: $s' \equiv 44(109) \pmod{73}$
$s' \equiv \underline{51}$

25: $s' \equiv 44(25) \pmod{73}$
$s' \equiv \underline{5}$

34: $s' \equiv 44(34) \pmod{73}$
$s' \equiv \underline{36}$

(3) Now solve knapsack problems using secret sequence, noting that $s' \equiv 44s \pmod{73}$, $s' \equiv 44(b_1 x_1 + \dots b_5 x_5)$, $b_i = a a_i$, a = multiplier, so $s' \equiv 44 a a_1 x_1 + \dots + 44 a a_5 x_5$, and since

$44a \equiv 1 \pmod{73}$, Then, $S' \equiv a_1 x_1 + \ldots + a_5 x_5$, where x_i is The binary code of the plaintext letter.

$\therefore S' = 11, 3, 54, 51, 5, 36$

$a_1, a_2, a_3, a_4, a_5 = 1, 3, 5, 11, 35$

$\therefore 11: \quad 11 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = x_2 = x_3 = 0, \ x_4 = 1, \ x_5 = 0$

$\therefore \ 00010 \Rightarrow \underline{\underline{C}}$

$3: \ 3 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = 0, \ x_2 = 1, \ x_3 = x_4 = x_5 = 0$

$\therefore 01000 \Rightarrow \underline{I}$

$54: 54 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = 0, \ x_2 = x_3 = x_4 = x_5 = 1$

$\therefore 01111 \Rightarrow \underline{P}$

$51: 51 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = x_2 = 0, \ x_3 = x_4 = x_5 = 1$

$\therefore 00111 \Rightarrow \underline{H}$

$5: 5 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = x_2 = 0, \ x_3 = 1, \ x_4 = x_5 = 0$

$\therefore 00100 \Rightarrow \underline{E}$

$36: 36 = x_1 + 3x_2 + 5x_3 + 11x_4 + 35x_5$

$\therefore x_1 = 1, \ x_2 = x_3 = x_4 = 0, \ x_5 = 1$

$\therefore 10001 \Rightarrow \underline{R}$

$\therefore$ CIPHER

19. A user of the knapsack cryptosystem has a private key consisting of the superincreasing sequence 2, 3, 7, 13, 27, modulus $m = 60$, and multiplier $a = 7$.

(a) Find the user's listed public key

$7(2) = 14$

$7(3) = 21$

$7(7) = 49$

$7(13) = 91 \equiv 31 \pmod{60}$

$7(27) = 189 \equiv 9 \pmod{60}$

$\therefore$ 14, 21, 49, 31, 9

(b) With the aid of the public key, encrypt the message: SEND MONEY.

First convert to binary equivalent:

SEND $\Rightarrow$ 10010 00100 01101 00011
MONEY $\Rightarrow$ 01100 01110 01101 00100 11000

The public key has 5 terms, so need blocks of 5 binary digits, which in this case is each letter (represented by 5 digits).

$\therefore$ $10010 \Rightarrow [1,0,0,1,0]\cdot[14,21,49,31,9] = 14 + 31 = 45$
$00100 \Rightarrow [0,0,1,0,0]\cdot[14,21,49,31,9] = 49$
$01101 \Rightarrow [0,1,1,0,1]\cdot[14,21,49,31,9] = 21 + 49 + 9 = 79$
$00011 \Rightarrow [0,0,0,1,1]\cdot[14,21,49,31,9] = 31 + 9 = 40$
$01100 \Rightarrow [0,1,1,0,0]\cdot[14,21,49,31,9] = 21 + 49 = 70$
$01110 \Rightarrow [0,1,1,1,0]\cdot[14,21,49,31,9] = 21 + 49 + 31 = 101$
$01101 \Rightarrow [0,1,1,0,1]\cdot[14,21,49,31,9] = 21 + 49 + 9 = 79$
$00100 \Rightarrow [0,0,1,0,0]\cdot[14,21,49,31,9] = 49$
$11000 \Rightarrow [1,1,0,0,0]\cdot[14,21,49,31,9] = 14 + 21 = 35$

$\therefore$ 45, 49, 79, 40, 70, 101, 79, 49, 35