MCS 425 Midterm Exam Solutions — Spring 2008

1. [4 points] An affine cipher $E_{\alpha,\beta}(x) = \alpha x + \beta \pmod{26}$ encrypts plaintext `er` as ciphertext `J*`, where `*` represents some ciphertext letter. Note the 26 letters correspond to the integers {0,1,...,25} as follows:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z

a) [3 points] What is `*`, i.e., what is the encryption of `r`?

From $E_{\alpha,\beta}$(**e**) = **J** and $E_{\alpha,\beta}$(**r**) = *****, we obtain

$$4\alpha + \beta \equiv 9 \pmod{26},$$
$$17\alpha + \beta \equiv * \pmod{26}.$$

Subtracting the first equation from the second gives

$$13\alpha \equiv * - 9 \pmod{26}.$$

Since $gcd(\alpha, 26) = 1$, α must be odd, i.e., $\alpha \equiv 1 \pmod 2$. It follows that $13\alpha \equiv 13 \pmod{26}$. Then $* \equiv 9 + 13\alpha \equiv 9 + 13 \equiv 22$. Thus **r** is encrypted to **W**.

b) [1 points] Could the cipher described above encrypt `b` as `C`? Why or why not?

Yes, it could. To see this, we have to show that the simultaneous equations

$$4\alpha + \beta \equiv 9 \pmod{26},$$
$$17\alpha + \beta \equiv 22 \pmod{26},$$
$$\alpha + \beta \equiv 2 \pmod{26},$$

have a solution.

The second equation follows from the first, so we can ignore it. Subtracting the third equation from the first gives

$$3\alpha \equiv 7 \pmod{26}.$$

Thus $\alpha \equiv 3^{-1}7 \equiv 9\cdot 7 \equiv 63 \equiv 11 \pmod{26}$. From the third equation,

$$\beta \equiv 2 - \alpha \equiv 2 - 11 \equiv -9 \equiv 17 \pmod{26}.$$

Thus there is a solution, $\alpha \equiv 11 \pmod{26}$ and $\beta \equiv 17 \pmod{26}$.

2. [5 points] Use the fact that

$$903^2 \equiv 481^2 \pmod{36503}$$

to produce a nontrivial factorization of 36503. Show your work, and use only methods applicable even with very large integers.

Note $903 \not\equiv \pm 481 \pmod{36503}$, so by a major theorem proven in class,

$$36503 = gcd(36503,\ 903-481)\cdot gcd(36503,\ 903+481)$$

provided that one (and hence both) of 481 and 903 are relatively prime to 36503.

$gcd(36503,\ 903-481) = gcd(36503,\ 422)$ is computed as follows:

$$36503 = 86\cdot 422 + 211$$
$$422 = 2\cdot 211 + 0$$

So $gcd(36503,\ 422) = 211$. $36503/211 = 173$, so **$36503 = 211\cdot 173$**.

3. [6 points] In this problem, show all your work, and use only techniques that can be used even with very large integers.

a) [2 points] Show that one of 3 or 5 is a quadratic residue mod 23, and the other is a nonresidue.

$(23-1)/2 = 11$. a is a quadratic residue mod 23 if and only if $a^{11} \equiv 1 \pmod{23}$.

$3^2 \equiv 9 \pmod{23}$
$3^{2^2} \equiv 9^2 \equiv 81 \equiv 12 \pmod{23}$
$3^{2^3} \equiv 12^2 \equiv 144 \equiv 6 \pmod{23}$
$3^{11} \equiv 3^{2^3}\cdot 3^2\cdot 3 \equiv 6\cdot 9\cdot 3 \equiv 162 \equiv 1 \pmod{23}$
So 3 is a quadratic residue mod 23.

$5^2 \equiv 25 \equiv 2 \pmod{23}$
$5^{2^2} \equiv 2^2 \equiv 4 \pmod{23}$
$5^{2^3} \equiv 4^2 \equiv 16 \pmod{23}$
$5^{11} \equiv 5^{2^3}\cdot 5^2\cdot 5 \equiv 16\cdot 2\cdot 5 \equiv 160 \equiv -1 \pmod{23}$
So 5 is a non-residue mod 23.

b) [2 points] Compute the square roots of 3 or 5 (the one that is a residue) mod 23.

Since $23 \equiv 3 \pmod 4$, and since we know that 3 is a quadratic residue mod 23, the square roots of 3 mod 23 must be $\pm 3^{(23+1)/4} = \pm 3^6$. Using the values of 3^2 and 3^{2^2} above, we compute $3^6 \equiv 3^{2^2}\cdot 3^2 \equiv 12\cdot 9 \equiv 108 \equiv 16 \pmod{23}$.

So the square roots of 3 mod 23 are **±16**. (They may also be written as **±7**.)

c) [2 points] Using only your result in part (a), and without performing any more computation, decide whether 15 is a quadratic residue mod 23.

We know that (*residue*)·(*non-residue*) = (*non-residue*). Since 3 is a residue mod 23 and 5 is a non-residue, 15 is a non-residue mod 23.

4. [5 points] Show how to compute a^{75} (mod m) using only 9 modular multiplications. Show where each multiplication is used.

Note $75 = (1001011)_2 = 2^6 + 2^3 + 2^1 + 2^0$

$$\left.\begin{array}{ll}
a_1 \equiv a^2 \pmod{m} & (a_1 \equiv a^{2^1}) \\
a_2 \equiv a_1^2 \pmod{m} & (a_2 \equiv a^{2^2}) \\
a_3 \equiv a_2^2 \pmod{m} & (a_3 \equiv a^{2^3}) \\
a_4 \equiv a_3^2 \pmod{m} & (a_4 \equiv a^{2^4}) \\
a_5 \equiv a_4^2 \pmod{m} & (a_5 \equiv a^{2^5}) \\
a_6 \equiv a_5^2 \pmod{m} & (a_6 \equiv a^{2^6})
\end{array}\right\} \text{6 multiplications}$$

$$\left.\begin{array}{ll}
a^{75} \equiv a_6\, a_3\, a_1\, a \pmod{m} & (a^{75} \equiv a^{2^6 + 2^3 + 2^1 + 2^0} \\
 & \quad \equiv a^{2^6} a^{2^3} a^{2^1} a^{2^0})
\end{array}\right\} \text{3 multiplications}$$

5. [5 points] In the circuit below,

a) [1.7 points] What is the output of the 5×4 S-box? _____1101__________

b) [1.7 points] What is the output of the XOR-box? _____1110__________

c) [1.6 points] What is the output of the 4×4 S-box? _____0101__________