**Mathematics 124–The Art and Science of Secret Writing**
**Winter 2009 (200910)**
**Final Exam Solutions**

**Instructor:** Michael Kozdron

**1.** If we write the ciphertext in three columns with eleven rows, then we have

```
DTG
IHO
LEO
IMD
GOF
ETO
NHR
CET
ERU
ION
SFE
```

We can now read down the columns to conclude that the plaintext is `DILIGENCE IS THE MOTHER OF GOOD FORTUNE`.

**2.** If the key matrix is

$$A = \begin{bmatrix} 11 & 18 \\ 12 & 17 \end{bmatrix},$$

then $\det(A) = 11 \cdot 17 - 18 \cdot 12 = -29 = 23 \,\mathrm{MOD}\, 26$. Since $23^{-1} = 17 \,\mathrm{MOD}\, 26$ (as can be easily checked), we conclude

$$A^{-1} = 17 \begin{bmatrix} 17 & -12 \\ -18 & 11 \end{bmatrix} = \begin{bmatrix} 289 & -204 \\ -306 & 187 \end{bmatrix} = \begin{bmatrix} 3 & 4 \\ 6 & 5 \end{bmatrix}.$$

We now compute

$$X = A^{-1}Y = \begin{bmatrix} 3 & 4 \\ 6 & 5 \end{bmatrix} \begin{bmatrix} 5 & 20 & 15 \\ 2 & 22 & 25 \end{bmatrix} = \begin{bmatrix} 27 & 192 & 195 \\ 30 & 190 & 185 \end{bmatrix} = \begin{bmatrix} 1 & 10 & 13 \\ 4 & 8 & 3 \end{bmatrix} \mathrm{MOD}\, 26.$$

Converting the numbers to their letter equivalents, we find the plaintext is `BE KIND`.

**3.** A nice description (including pictures) of the German Enigma machine may be found at `http://en.wikipedia.org/wiki/Enigma_machine`. An Enigma machine consisted of five primary cryptographic components: (i) a *plugboard* which could contain from zero to thirteen dual-wired cables; (ii) three ordered (left to right) *rotors* which wired twenty-six input contact points to twenty-six output contact points positioned on alternate faces of a disc; (iii) twenty-six *serrations* around the periphery of the rotors which allowed the operator to specify an initial rotational position for the rotors; (iv) a moveable *ring* on each of the rotors which controlled the rotational behavior of the rotor immediately to the left by means of a notch; and (v) a *reflector* half-rotor (which did not in fact rotate) to fold inputs and outputs back onto the same face of contact points.

**4. (a) F** Two numbers whose greatest common divisor is 1 are relatively prime, but neither of them need themselves be prime. For instance, 12 and 25 are relatively prime, although neither $12 = 2^2 \cdot 3$ nor $25 = 5^2$ are prime.

**4. (b) F** Although `E` is the most frequently occurring English letter, this is averaged over many texts. In a particular piece of text, it need not be true that `E` is the most common letter. Consider, for instance, the text given in Problem 11 of this exam: `T` is the most frequently occurring letter in it.

**4. (c) F** A scytale implements a transposition cipher.

**4. (d) T** This statement is true. If an efficient method for factoring very large numbers is found, then RSA would no longer be a secure means of encryption.

**4. (e) F** In a transposition cipher, the letters of the plaintext are rearranged to form the ciphertext.

**4. (f) T** This statement is true. Public key cryptosystems tend to run more slowly on computers than secret-key systems.

**5. (a)** Writing 124 in terms of powers of 2 we find $124 = 64 + 32 + 16 + 8 + 4$ so that its binary representation is 1111100.

**5. (b)** Using 1111100 as the key, we find

| | | | | |
|---|---|---|---|---|
| cipher | 0110000 | 0110011 | 0101111 | 0101000 |
| key | 1111100 | 1111100 | 1111100 | 1111100 |
| plain | 1001100 | 1001111 | 1010011 | 1010100 |

and so if we now convert each of the 7-bit strings to decimal, then

$$\begin{aligned} 1001100 &= 64 + 8 + 4 = 76, \\ 1001111 &= 64 + 8 + 4 + 2 + 1 = 79, \\ 1010011 &= 64 + 16 + 2 + 1 = 83, \\ 1010100 &= 64 + 16 + 4 = 84. \end{aligned}$$

From the ASCII chart, we find the plaintext reads `LOST`.

**6. (a)** Using the Euclidean algorithm we find

$$\begin{aligned} 131071 &= 64 \cdot 2047 + 63 \\ 2047 &= 32 \cdot 63 + 3 \\ 63 &= 2 \cdot 31 + 1 \end{aligned}$$

so that $\gcd(131071, 2047) = 1$. The extended Euclidean algorithm therefore implies

$$\begin{aligned} 131071 - 64 \cdot 2047 &= 63 \\ 2047 &= 32 \cdot 63 + 31 \\ 0 &= -63 + 2 \cdot 31 + 1 \end{aligned}$$

so that

$$65 \cdot 131071 - 4162 \cdot 2047 = 1.$$

**6. (b)** Since $\gcd(131071, 2047) = 1$, we know that $2047^{-1} \,\text{MOD}\, 131071$ exists. From **(a)**, we have

$$2047^{-1} \equiv -4162 \equiv 126909 \pmod{131071},$$

so that $2047^{-1} \,\text{MOD}\, 131071 = 126909$.

**6. (c)** From **(a)**, we have $65 \cdot 131071 - 4162 \cdot 2047 = 1$ so one pair of integers that works is $(65, -4162)$. In order to find another pair we can simply add-and-subtract $131071 \cdot 2047$ from the left side of the equation. That is, if $65 \cdot 131071 - 4162 \cdot 2047 = 1$, then

$$65 \cdot 131071 + 131071 \cdot 2047 - 4162 \cdot 2047 - 131071 \cdot 2047 = 1.$$

We can simplify this:

$$(65 + 2047) \cdot 131071 - (4162 + 131071) \cdot 2047 = 1,$$

and so

$$2112 \cdot 131071 - 135233 \cdot 2047 = 1.$$

That is, another pair of integers is $(2112, -135233)$. Similarly, $(-1982, 126909)$ works.

**7. (a)** Fermat's Little Theorem tells us that $a^p \equiv a \pmod{p}$. Since 17 is prime, we conclude that $7^{17} \equiv 7 \pmod{17}$. Hence,

$$7^{18} \equiv 7^{17} \cdot 7 \equiv 7 \cdot 7 \equiv 49 \equiv 15 \pmod{17}$$

so that $7^{18} \,\text{MOD}\, 17 = 15$.

**7. (b)** Fermat's Little Theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$. Since 13 is prime, we conclude that $6^{12} \equiv 1 \pmod{13}$. We now write $84 = 7 \cdot 12$ so that

$$6^{84} \equiv (6^{12})^7 \equiv 1^7 \equiv 1 \pmod{13}.$$

Hence, $6^{84} \,\text{MOD}\, 13 = 1$.

**7. (c)** Since $6^{84} \equiv 1 \pmod{13}$, we see that

$$6^{87} \equiv 6^{84} \cdot 6^3 \cdot 6^3 \equiv 216 \equiv 8 \pmod{13}$$

and so $6^{87} \,\text{MOD}\, 13 = 8$.

**7. (d)** Since $51 = 3 \cdot 17$ is the product of primes, we can use Euler's Theorem. We write 163 in terms of $2 \cdot 16 = 32$ as follows: $163 = 5 \cdot 32 + 4$. Since Euler's Theorem tells us that

$$5^{161} \equiv 5^{5 \cdot 32 + 1} \equiv 5 \pmod{51},$$

we conclude

$$5^{163} \equiv 5^{161} \cdot 5^2 \equiv 5 \cdot 5^2 \equiv 125 \equiv 23 \pmod{51},$$

and so $5^{163} \,\text{MOD}\, 51 = 23$.

**8.** In order to determine $a$ and $b$ we begin by finding the numerical equivalents of the letters in `FAME` and `RIOK`. That is,

| F | A | M | E | | R | I | O | K |
|---|---|---|---|---|---|---|---|---|
| 5 | 0 | 12 | 4 | and | 17 | 8 | 14 | 10 |

Since the `F` in `FAME` corresponds with the `R` in `RIOK`, we know that $E(5) = (5a + b) \,\mathrm{MOD}\, 26 = 17$ and since the `A` in `FAME` corresponds with the `I` in `RIOK` we know that $E(0) = b \,\mathrm{MOD}\, 26 = 8$. Thus, from this second piece of information, we immediately conclude that $b = 8$. Therefore, we also know that $a$ satisfies

$$(5a + 8) = 17 \,\mathrm{MOD}\, 26 \quad \text{and so} \quad 5a = 9 \,\mathrm{MOD}\, 26.$$

We now need to solve for $a$. The easy way is to notice that $5 \cdot 7 - 9 = 35 - 9 = 26$ and so $a = 7$. Hence we conclude that the required $a$ and $b$ are $a = 7$, $b = 8$ so that $E(x) = (7x + 8) \,\mathrm{MOD}\, 26$ is the affine cipher used.

**9. (a)** Alice's public modulus is $m = pq = 31961$.

**9. (b)** Alice's decryption key $d$ is given by $d = e^{-1} \,\mathrm{MOD}\, n$ where $n = (p-1)(q-1) = 30900$. Since $e = 2377$, we need to compute $2377^{-1} \,\mathrm{MOD}\, 30900$. This can be done using the extended Euclidean algorithm. That is,

$$\begin{aligned} 30900 - 12 \cdot 2377 &= 2376 \\ 2377 &= 2376 + 1 \end{aligned}$$

so that

$$-30900 + 13 \cdot 2377 = 1.$$

Hence, Alice's decryption key is $d = 2377^{-1} \,\mathrm{MOD}\, 30900 = 13$.

**9. (c)** If Alice receives the ciphertext message $y$ from Bob, then the plaintext is $x = y^d \,\mathrm{MOD}\, m$. Thus, Alice needs to compute

$$103^{13} \,\mathrm{MOD}\, 31961.$$

This can be done with repeated exponentiation. That is,

$$\begin{aligned} 103^2 &\equiv 10609 \pmod{31961} \\ 103^4 &\equiv 16200 \pmod{31961} \\ 103^8 &\equiv 8229 \pmod{31961} \end{aligned}$$

so that

$$104^{13} \equiv 8229 \cdot 16200 \cdot 103 \equiv 16601 \cdot 16200 \equiv 16346 \pmod{21961}.$$

In other words, the plaintext is $x = 16346$. If we now write

$$16346 = 25 \cdot 26^2 + 4 \cdot 26 + 18,$$

then we can read Bob's message which is `YES`.

**10.** The key that Alice and Bob agree upon is

$$k = s^{ab} \operatorname{MOD} p = 31^{143 \cdot 83} = 31^{11869} \operatorname{MOD} 5927.$$

We can now use Fermat's Little Theorem, namely $a^p \equiv a \pmod{p}$, to reduce the exponent. That is,

$$31^{5927} \equiv 31 \pmod{5927}.$$

Since we can write $11869 = 2 \cdot 5927 + 15$, we have

$$31^{11869} \equiv 31^{2 \cdot 5927 + 15} \equiv 31^{5927} \cdot 31^{5927} \cdot 31^{15} \equiv 31 \cdot 31 \cdot 31^{15} \equiv 31^{17} \pmod{5927}.$$

We can now compute $k$ by repeated exponentiation; that is,

$$\begin{aligned} 31^2 &\equiv 961 \pmod{5927} \\ 31^4 &\equiv 4836 \pmod{5927} \\ 31^8 &\equiv 4881 \pmod{5927} \\ 31^{16} &\equiv 3548 \pmod{5927} \end{aligned}$$

and so

$$31^{17} \equiv 31 \cdot 31^{16} \equiv 31 \cdot 3548 \equiv 3302 \pmod{5927}.$$

Thus, $k = 3302$.

**11.** Since `B` and `M` are the most frequent letters, we suspect that they correspond to {`E`, `T`, `N`, `O`, `R`, `I`, `A`, `S`}. If we now notice that the first three letters in the ciphertext are `BPM`, we strongly suspect that `B` corresponds with `T` while `M` corresponds with `E`. Working with the numerical equivalents, we see that both of our guesses corresponds to a shift of +18. If we then apply a shift of +18 to all of the letters of the ciphertext, we arrive at the required plaintext, namely, `THE MOST CERTAIN WAY TO SUCCEED IS ALWAYS TO TRY JUST ONE MORE TIME`.