Solutions to Math 135 Final Exam (Summer 2006)

1. (a) Alice's public modulus is $m = p \cdot q = 23 \cdot 37 = 851$.

(b) Converting the message BAT to base twenty-six gives $\texttt{BAT} = 1 \cdot 26^2 + 0 \cdot 26 + 19 = 695$. Therefore, since the RSA encryption function is $E(x) = x^e \,\mathrm{MOD}\, m$, Bob's ciphertext is given by $y = E(695) = 695^{13} \,\mathrm{MOD}\, 851$. In order to compute the modular exponential, we repeatedly square:

$$\begin{aligned} 695^2 &\equiv 508 \pmod{851} \\ 695^4 &\equiv 508^2 \equiv 211 \pmod{851} \\ 695^8 &\equiv 211^2 \equiv 269 \pmod{851}. \end{aligned}$$

We then conclude that

$$695^{13} \equiv 695^8 \cdot 695^4 \cdot 695 \equiv 269 \cdot 211 \cdot 695 \equiv 593 \cdot 695 \equiv 251 \pmod{851}.$$

Thus, the ciphertext is $y = 851$ which converted to base twenty-six reads

$$251 = 9 \cdot 26 + 17 = \texttt{JR}.$$

(c) Alice's decryption key is given by $d = e^{-1} \,\mathrm{MOD}\, n$ where $n = (p-1) \cdot (q-1)$. We find $n = 22 \cdot 36 = 792$ so that $d = 13^{-1} \,\mathrm{MOD}\, 792$. In order to calculate this modular inverse, we use the extended Euclidean algorithm so that

$$\begin{aligned} 792 &= 60 \cdot 13 + 12 \\ 13 &= 12 + 1. \end{aligned}$$

Back substitution therefore gives $-792 + 61 \cdot 13 = 1$ from which we conclude that $d = 13^{-1} \,\mathrm{MOD}\, 792 = 61$.

(d) The RSA decryption function for Alice is given by $D(y) = y^d \,\mathrm{MOD}\, m$ so that Bob's plaintext message is $x = D(625) = 625^{61} \,\mathrm{MOD}\, 851$. In order to compute the modular exponential, we repeatedly square:

$$\begin{array}{ll} 625^2 \equiv 16 \pmod{851} & 625^{16} \equiv 9^2 \equiv 81 \pmod{851} \\ 625^4 \equiv 16^2 \equiv 256 \pmod{851} & 625^{32} \equiv 81^2 \equiv 604 \pmod{851}. \\ 625^8 \equiv 256^2 \equiv 9 \pmod{851} & \end{array}$$

We then conclude that

$$625^{61} \equiv 625^{32} \cdot 625^{16} \cdot 625^8 \cdot 625^4 \cdot 625 \equiv 604 \cdot 81 \cdot 9 \cdot 256 \cdot 625 \equiv 784 \pmod{851}.$$

Thus, the plaintext is $x = 784$ which converted to base twenty-six reads

$$784 = 1 \cdot 26^2 + 4 \cdot 26 + 4 = \texttt{BEE}.$$

2. (a) Given the prime factorization of a and b, we can read off their greatest common divisor which is $\gcd(a, b) = 2^3 \cdot 23 \cdot 97^2$.

(b) Recall that Fermat's Little Theorem says $a^p \equiv a \pmod{p}$ for all primes p. Since 2833 is prime, we conclude that

$$4^{2834} \equiv 4^{2833} \cdot 4 \equiv 4 \cdot 4 \equiv 16 \pmod{2833}.$$

Hence, $4^{2834} \,\mathrm{MOD}\, 2833 = 16$.

(c) Since $23 \cdot 523 - 124 \cdot 97 = 1$, we find $97^{-1} \equiv -124 \pmod{523}$ so that $97^{-1} \operatorname{MOD} 523 = 399$.

(d) The security of RSA rests on the computationally challenging problem of factoring a large number. Since $m = p \cdot q$ where p and q are prime and m is made public, an RSA encrypted message can be cryptanalyzed *if* m can be factored into its prime factors p and q. Currently computing power is not able to accomplish this task in real time when p and q are on the order of 100 digits each.

(e) Recall that for Friedman's test, the estimated keyword length is given by

$$k = \frac{0.0265n}{(0.065 - I) + n(I - 0.0385)}$$

where I is the index of coincidence. Hence, if $n = 10000$ and $I = 0.05$, then

$$k = \frac{0.0265 \cdot 10000}{(0.065 - 0.05) + 10000(0.05 - 0.0385)} \approx 2.3$$

and if $n = 10000$ and $I = 0.05$, then

$$k = \frac{0.0265 \cdot 10000}{(0.065 - 0.041) + 10000(0.041 - 0.0385)} \approx 10.6.$$

Thus, we conclude that the text with index of coincidence 0.0414 is likely to correspond to a longer keyword.

(f) We can write the hexadecimal number FB in decimal as $FB = 15 \cdot 16 + 11 = 251$. Therefore, its base twenty-six representation is $251 = 9 \cdot 26 + 17 =$ `JR`. (See Problem **1. (b)** again!)

3. (a) In order to determine the key, we need to calculate $k = s^{ab} \operatorname{MOD} p = 29^{167 \cdot 80} \operatorname{MOD} 6679 = 29^{13360} \operatorname{MOD} 6679$. Since $13360 = 2 \cdot 6679 + 2$, we can use Fermat's Little Theorem to conclude

$$29^{13360} \equiv 29^{2 \cdot 6679} \cdot 29^2 \equiv 29^2 \cdot 29^2 \equiv 29^4 \equiv 5986 \pmod{6679}.$$

Therefore, $k = 5986$.

(b) Since $k = 4096 + 1024 + 512 + 256 + 64 + 32 + 2 = 2^{12} + 2^{10} + 2^9 + 2^8 + 2^6 + 2^5 + 2$ we find that the binary representation of k is 1011101100010.

4. The correct answers are:

(a) T If a and b are distinct primes, then a and b are relatively prime.

(b) F William Friedman and Francis Bacon were co-workers during World War II in breaking the Enigma cipher.

(c) T A scytale is a device that implements a type of transposition substitution.

(d) F If an efficient method for calculating modular exponentials were found, then RSA would no longer be a secure means of encryption.

(e) F A principle of modern cryptography is that the security of a cipher system rests on keeping the method of encipherment secure.

(f) **F** Fermat's Little Theorem was discovered in 1970 while researchers were looking for an asymmetric cryptosystem.

(g) **F** The probability of randomly selecting the letter `E` from a sample of English text is approximately $\frac{1}{26}$.

(h) **T** The World War II Enigma cryptosystem relied on both transposition and substitution for its cipher.

5. Converting both the ciphertext and keyword to their numerical equivalents, and subtracting modulo 26 gives

y	18	5	2	23	25	24	13	18	9
k	18	20	17	4	18	20	17	4	18
$y-k$	0	-15	-15	19	7	4	-4	14	-9
$(y-k)\,\mathrm{MOD}\,26$	0	11	11	19	7	4	22	14	17

y	5	20	22	18	12	10	4	24	24
k	20	17	4	18	20	17	4	18	20
$y-k$	-15	3	18	0	-8	-7	0	6	4
$(y-k)\,\mathrm{MOD}\,26$	11	3	18	0	18	19	0	6	4

and so converting back gives the plaintext `ALL THE WORLD'S A STAGE`.

6. In order to determine a and b we begin by finding the numerical equivalents of the letters in `CRYPTO` and `AVKNDW`. That is,

C	R	Y	P	T	O	and	A	V	K	N	D	W
2	17	24	15	19	14		0	21	10	13	3	22

Since the `C` in `CRYPTO` corresponds with the `A` in `AVKNDW`, we know that $E(2) = (2a + b)\,\mathrm{MOD}\,26 = 0$ and since the `R` in `CRYPTO` corresponds with the `V` in `AVKNDW` we know that $E(17) = (17a + b)\,\mathrm{MOD}\,26 = 21$. Thus, we need to solve the two congruences

$$\begin{aligned} 17a + b &\equiv 21 \pmod{26} \\ 2a + b &\equiv 0 \pmod{26} \end{aligned}$$

for a and b. If we subtract $2a + b \equiv 0 \pmod{26}$ from $17a + b \equiv 21 \pmod{26}$, then we see that $15a \equiv 21 \pmod{26}$. Since $15^{-1} \equiv 7 \pmod{26}$, we conclude that $a \equiv 147 \equiv 17 \pmod{26}$. Substituting back into $2a + b \equiv 0 \pmod{26}$ for a gives $34 + b \equiv 0 \pmod{26}$ and so $b \equiv -34 \equiv 18 \pmod{26}$. Hence we conclude that the required a and b are $a = 17$, $b = 18$ so that $E(x) = (17x + 18)\,\mathrm{MOD}\,26$ is the affine cipher used.

7. **(a)** A trusted authority (TA) is an entity on a network (usually another computer) that is responsible for verifying the identities of users, and distributing cryptographic keys to users. The TA could simply be a computer which is used to pre-distribute keys to all $C(n, 2)$ pairs on an n-person network. A more complicated scheme could be used such as Kerberos where each user shares a secret key with the TA, and through this gets a unique session key to communicate with other users on the network.

(b) The phrase 128-bit encryption is used to refer to the Advanced Encryption Standard (AES) which is a block cipher adopted as an encryption standard by the US government. AES has a fixed block size of 128 bits (and a key size of either 128, 192, or 256 bits).

(c) A Secure Sockets Layer (SSL) certificate is issued by a certificate authority (CA) such as VeriSign and consists of both a public key and private key. In essence, the CA is acting as the TA. When a client's Web browser points to a secured domain, a SSL handshake authenticates the server (the client's browser reads the certificate to verify the server's identity) and establishes an encryption method and unique session key.

(d) Server authentication allows you to confirm a Web server's identity. This is done by your browser checking whether or not a server's certificate and public key are valid and have been digitally signed by a certificate authority such as VeriSign. Encryption, of course, refers to the intent of the two parties to hide the content of their communications. In modern secure communications, RSA is commonly used for the key exchange and then a symmetric cipher such as AES is used for the rest of the message.

8. (a) Given 6 letters, there are

$$C(6,2) = \frac{6!}{4!\,2!} = 15$$

ways to select a pair of distinct letters.

(b) One way to count the number of possible ways to select the two distinct pairs of distinct letters is to count how to select the four letters that will comprise the two pairs, and then to count how many possible pairs can be made from those four letters. There are $C(6,4)$ ways to select 4 letters from 6. Given 4 letters, there are 3 ways to make two pairs. (Note that given 4 letters, once the first letter is chosen, there are 3 letters available to complete the first pair. The remaining two letters automatically comprise the second pair.) By the multiplication principle, the number of possible ways to select the two distinct pairs of distinct letters is

$$C(6,4)\cdot 3 = \frac{6!}{2!\,4!}\cdot 3 = 45.$$

9. (a) If $A = \begin{bmatrix} 4 & 3 \\ 5 & 10 \end{bmatrix}$ then $\det(A) = 4\cdot 10 - 3\cdot 5 = 25$. Since $25x \equiv 1 \pmod{26}$ is clearly satisfied by $x \equiv -1 \equiv 25 \pmod{26}$, we conclude $25 = \det(A)^{-1}\,\mathrm{MOD}\,26$. Therefore,

$$A^{-1} = 25\begin{bmatrix} 10 & -3 \\ -5 & 4 \end{bmatrix} = \begin{bmatrix} 250 & -75 \\ -125 & 100 \end{bmatrix} = \begin{bmatrix} 16 & 3 \\ 5 & 22 \end{bmatrix} \mathrm{MOD}\,26.$$

(b) If the ciphertext is `OO`, then converting to numerical equivalents gives $Y = \begin{bmatrix} 14 \\ 14 \end{bmatrix}$ and so we must find the plaintext X which satisfies $AX = Y$, or

$$\begin{bmatrix} 4 & 3 \\ 5 & 10 \end{bmatrix}\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 14 \\ 14 \end{bmatrix}.$$

Since A is invertible, we conclude that $X = A^{-1}Y$ so that

$$\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 16 & 3 \\ 5 & 22 \end{bmatrix}\begin{bmatrix} 14 \\ 14 \end{bmatrix} = \begin{bmatrix} 266 \\ 378 \end{bmatrix} = \begin{bmatrix} 6 \\ 14 \end{bmatrix} \mathrm{MOD}\,26.$$

Therefore, converting the numerical equivalents back to letters gives the plaintext as `GO`.