MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough

Solutions to the Midterm Test (March 5, 2011)

YOUR NAME:

DO NOT OPEN THIS BOOKLET UNTIL INSTRUCTED TO DO SO.

INSTRUCTIONS:

There are 6 numbered pages in this exam. Make sure that, at the start of the exam, this booklet has all its pages. Write your name on each page.

Try to answer all questions, indicating all the steps you are making. Show your work. However, verbal explanations don't have to be lengthy.

You can use the back of the pages both for side calculations and for the final solutions. Don't use extra paper for the final solutions.

You have 115 minutes.

The maximum possible score is 40 points.

Calculators are permitted, but the extended Euclidean algorithm and the matrix inversion formula have to be written out, if they are needed in a problem.

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

q	r	s	t	u	v	w	x	y	z
16	17	18	19	20	21	22	23	24	25

Warning: for RSA, a is 01, b is 02, etc.

Problem 1. $(1 + 2 + 2 + 4$ **points)**

(a) Find $\gcd(2^{345}9^4 10^{17}33^{55},\ 2^{34}3^{50}11^{11}50^3)$.

Solution. Looking at prime factors, $\gcd(2^{345}3^8 2^{17}5^{17}3^{55}11^{55},\ 2^{34}3^{50}11^{11}2^3 5^6) = 2^{37}3^{50}5^6 11^{11}$.

(b) Find $\gcd(24\,542\,107,\ 23\,758\,901)$.

Solution. Euclidean algorithm. $24\,542\,107 = 1 \times 23\,758\,901 + 783\,206$. Then $23\,758\,901 = 30 \times 783\,206 + 262\,721$. Then $783\,206 = 2 \times 262\,721 + 257\,764$. Then $262\,721 = 1 \times 257\,764 + 4957$. Then $257\,764 = 52 \times 257\,764 + 0$, hence stop. So, gcd $= 4957$.

(c) Find a nontrivial factor of $6\,482\,107$ using Fermat's factorization trick.

Solution. The trick is that if $\sqrt{x + i^2} = k$ is an integer, then $x = (k - i)(k + i)$. Let's try:
$\sqrt{6\,482\,107 + 1} = 2545.998\ldots$, not an integer.
$\sqrt{6\,482\,107 + 4} = 2545.999\ldots$, not an integer.
$\sqrt{6\,482\,107 + 9} = 2546$, an integer, great. So, $6\,482\,107 = 2543 \times 2549$.

(d) Show that 561 is a "little Fermat" pseudoprime for base 2.

Solution. This means that $2^{560} \equiv 1 \pmod{561}$, but 561 is not a prime. It is indeed composite, since divisible by 3. To calculate 2^{560}, let's do repeated squaring (or sometimes a higher power when it fits into the calculator). $560 = 512 + 32 + 16$. Then, $2^{16} \equiv 460 \pmod{561}$, then $2^{32} \equiv 460^2 \equiv 103 \pmod{561}$, then $2^{128} \equiv 103^4 \equiv 256 \pmod{561}$, then $2^{512} \equiv 256^4 \equiv 103 \pmod{561}$. Altogether, $560 \equiv 103 \times 103 \times 460 \equiv 1 \pmod{561}$, as it was claimed.

Problem 2. **($6 + 3$ points)**

(a) What are diffusion and confusion? Which of them are satisfied by Vigenère and DES? Explain briefly.

Solution. Diffusion means that each letter in the ciphertext depends on many letters in the plaintext, and vice versa. Equivalently, well, a bit more precisely, changing one letter in the plaintext changes the ciphertext completely, in an almost random-like fashion. Confusion is the same relation, just between the key and the ciphertext. (1+1 pt)

Vigeneré doesn't have either, since the repeated keyword is added to the plaintext letter-by-letter to get the ciphertext letters one-by-one. So, changing one letter in the plaintext changes only one letter in the ciphertext. Changing one letter in the key changes one letter in each block of the ciphertext, so one could say that many letters are changed, but not at all in a random-like manner. (Also in general, diffusion and confusion should always be judged within one block.) (1+1 pt)

DES has both properties. Change a letter in the plaintext. When that part gets inputed into an S-box, then the output of the S-box changes a lot (a design criterion for S-boxes). These changed bits will be transported into different places in the text, by expansions and permutations. Hence, in the next round (DES is done in round), they will be inputed into different S-boxes, changing each of these S-box outputs a lot. And so on. Round-by-round, more changes are generated, producing good diffusion if the number of rounds is high enough. Confusion works the same way, since the key is added to the plaintext before the S-boxes. (1+1 pt)

(b) What is an LFSR sequence? How can they be used in cryptography? Mention one advantage and one drawback of their use.

Solution. It is a sequence of numbers generated by a finite order linear recurrence relation, $x_n = c_1 x_{n-1} + \cdots + c_k x_{n-k}$, for some fixed $c_1, \ldots, c_k$, and an initial seed $x_1, \ldots, x_k$. Often it is taken mod 2, and then $x_i \in \mathbb{Z}_2$.

This is a fast and cheap way of generating a somewhat random-looking 0-1-sequence from a small seed. (The period of the resulting sequence can be $2^k - 1$ for an order k recursion.) Then this pseudo-random sequence can be used, e.g., as a key in a one-time pad or other cryptosystem.

The disadvantage is that it is not very random, hence not very secure: given a relatively short piece of the sequence, the recursion can be found easily, yielding the rest of the sequence.

Problem 3. (7 points) You have captured a long ciphertext, starting with $AA\ldots$, which was encrypted with a 2×2 Hill cipher (mod 26). You also know the first two letters of the plaintext: MN. (Sorry, it doesn't look like a very meaningful plaintext beginning, but let's assume that if you saw the entire plaintext, you would recognize its meaning. Maybe it's talking about Minnesota...) Incorporating this information, you perform a brute force search to find the key matrix. How large a keyspace do you still have to search through? (Warning: don't forget that the key matrix has to be invertible mod 26.)

Solution. If the key matrix is $K = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then the information we have is that

$$(12\ 13)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv (0\ 0) \pmod{26}.$$

This translates into the equations $12a + 13c \equiv 0$ and $12b + 13d \equiv 0 \pmod{26}$. Let's look at the first equation, and the second will be the same.

Clearly, a has to be divisible by 13, otherwise there is no solution for c. So $a \in \{0, 13\}$. If $a = 0$, then c would need to be even, but then the first column of K is all even, hence its determinant would be even, so it cannot be invertible mod 26, since gcd(even,26)$\neq$1. So, $a = 13$ must be. Then c could be any even number, so there are 13 choices for it. Altogether, there are 13 choices for (a, c). Similarly, there are 13 choices for (b, d). But, oops, in all these $13 \times 13 = 169$ choices, we have $a = b = 13$, which means that the determinant of the matrix will be divisible by 13, hence the matrix won't be invertible.

So, there is no admissible K, and you don't need to do any brute force search.

(Getting 169 is worth 6 pts, getting 4×169 is worth 4 pts. It is also possible to get "no good K" by a wrong argument, e.g., by messing up how Hill cipher acts on the plaintext; that would be worth 2 pts. It might also be possible to get the "no good K" result by a different and correct argument; that gets full credit, of course. Unfortunately, I changed something in this problem in the last minute to make it simpler, and with that, I messed it up.)

Problem 4. $(4 + 4$ **points)**

(a) Show that $x^4 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$.

Solution. If it is reducible, then the degree count could be $4 = 3 + 1$ or $4 = 2 + 2$ (or subcases of these, like $2 + 1 + 1$). If it has a degree 1 factor, then it also has a root. But $1^4 + 1 + 1 \equiv 0^4 + 0 + 1 \equiv 1 \pmod 2$, hence no roots. (Or one could check that it's not divisible by either x or $x + 1$.) So, let's try irreducible degree 2 factors. The degree two polynomials in $\mathbb{Z}_2[x]$ are x^2, $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$, but only the last one is irreducible. Long division gives $x^4 + x + 1 = (x^2 + x + 1)(x^2 + x) + 1$, hence this is not a factor, either.

(b) What is the multiplicative inverse of x^{15} in the field $\mathbb{Z}_2[x] \pmod{x^4 + x + 1}$?

Solution. Long division gives $x^{15} = (x^2 + x + 1)(x^{11} + x^8 + x^7 + x^5 + x^3 + x^2 + x + 1) + 1$, hence $x^{15} \equiv 1 \pmod{x^4 + x + 1}$ in $\mathbb{Z}_2[x]$. And the multiplicative inverse of 1 is just 1, of course.

Problem 5. **($5 + 2$ points)**

(a) The ciphertext 5859 was obtained with RSA using $n = 11413 = 101 \cdot 113$ and $e = 7467$. Find the plaintext (using $01 = a$, $02 = b$, etc.).

Solution. $\varphi(n) = 100 \times 112$, so want $d = 7467^{-1} \pmod{11200}$, the decryption exponent. Run the extended Euclidean algorithm: $11200 = 1 \times 7467 + 3733$, then $7467 = 2 \times 3733 + 1$, and stop, gcd=1. Now work backwards, $1 = 7467 - 2 \times 3733 = 7467 - 2(11200 - 7467) = 3 \times 7467 - 2 \times 11200$. Therefore, the inverse of 7467 is $d = 3$.

Now $5859^3 \equiv 1415 \pmod{11413}$, which translates to the plaintext *no*.

(b) Give a version of RSA that satisfies authentication and non-repudiation.

Solution. Besides Bob having a public key $k_B = (n_B, e_B)$, let also Alice have a public key $k_A = (n_A, e_A)$. Encryption and decryption with a key k will be denoted by E_k and D_k. In a public key cryptosystem like RSA, anyone can do E_{k_A}, but only Alice can do D_{k_A}.

If Alice wants to send the message m to Bob, she can send $E_{k_B}(D_{k_A}(m))$. Only Bob can take off the outside encryption, by applying D_{k_B}, so this is secure. He gets $D_{k_A}(m)$. Then he can apply E_{k_A} to $D_{k_A}(m)$ to get m. If applying E_{k_A} results in something meaningful, then it must have been something meaningful encrypted with D_{k_A}, but only Alice knows D_{k_A}. This proves to Bob (authentication) and to the world (non-repudiation) that Alice was the sender.

Note that $D_{k_A}(E_{k_B}(m))$ also achieves authentication and non-repudiation, in the same way as above, so that's a full solution, too. (And there could be further correct variations.) The issue with $D_{k_A}(E_{k_B}(m))$ that we mentioned in class is that Eve can take off D_{K_A} by applying the public E_{k_A}, which might be undesirable, e.g., if Bob is a professor, Alice and Eve are students, and m is the solution to a homework; in that case, Eve can send $E_{k_B}(m)$ (or $D_{k_{Eve}}(E_{k_B}(m))$) to Bob without knowing what m is.