MATC16 Cryptography and Coding Theory
Gábor Pete
University of Toronto Scarborough

Midterm Test (Feb 24, 2009) — Solutions

Problem 1. **(5×2 points)**

(a) What is a public key cryptosystem?

Solution: The encryption key is public (known to everyone), only the decryption key is kept private. It is computationally infeasible to find the decryption key from the known encryption key. With the public key, anyone can send an encrypted message to Bob.

(b) What is a private (symmetric) key cryptosystem?

Solution: Both the decryption and encryption keys must be kept private (among Alice and Bob), because they are easily computed from each other. (In fact, they are often actually the same, e.g., in DES). So the participants have to agree in the key over a secure channel beforehand (e.g., by personal meeting).

(c) What is a substitution cipher?

Solution: The key is a bijection from the alphabet to itself: each letter is substituted by another letter (same plaintext letter always becomes the same ciphertext letter).

(d) Define the non-repudiation requirement for a cryptosystem. Explain why standard symmetric key systems fail to satisfy it.

Solution: The ciphertext has enough information that uniquely identifies the sender: she cannot deny that she sent the message. In symmetric key systems, the receiver knows the sender's encryption key, hence could have produced the ciphertext himself.

(e) What is a one-time pad?

Solution: Assuming that the message is a binary sequence, generate a random binary sequence of the same length, this is the secret key, and add it bitwise to the plaintext to get the ciphertext. Decryption is adding the key again to the ciphertext. For a single use it's perfectly safe, since the ciphertext is a completely random binary sequence.

Problem 2. (3×3 **points**)

(a) In the Vigenère cryptosystem, if Alice first encrypts a plaintext with the keyword ALICE, then encrypts the resulting ciphertext with the keyword BOB, is that safer than encrypting only with ALICE?

Solution: Since the Least Common Multiple of 3 and 5 is 15, the combination is again just Vigenère, now with a length 15 keyword:

plaintext	x_1	x_2	x_3	x_4	x_5	x_6	x_7	...	x_{15}	x_{16}	x_{17}	...
1st keyword	A=0	L=11	I	C	E	A	L	...	E	A	L	...
2nd keyword	B=1	O=14	B	B	O	B	B	...	B	B	O	...
ciphertext	x_1+1	x_2+25	...							$x_{16}+1$	$x_{17}+25$	...

If we have a long ciphertext, this doesn't really increase security, since one can break the ciphertext with the usual methods against Vigenère. For short ciphertexts, though, it is a bit safer, since we need to do frequency analysis on every 15th letter, instead of every 5th letter, hence we have less data for each analysis, which makes the results less certain.

(b) How does a known plaintext attack work against Vigenère?

Solution: If the plaintext is $x_1x_2\ldots$, the ciphertext is $y_1y_2\ldots$, then the key is $k_1k_2\ldots$ with $k_i = y_i - x_i \pmod{26}$. This key is a periodic sequence, just repeating the keyword, so the keyword can be read off immediately. (Of course, the length of the texts should be at least a couple of times larger than the keyword length to recognize the period without doubt.)

(c) Summarize in two or three sentences how a ciphertext only attack works against Vigenère.

Solution: First displace the ciphertext by 1, 2, etc. letters, find which gives the largest number of coinciding letters, and that should be the keyword length.
(Note for maximalists: This is unsafe for displacements 1 and 2, because of the correlations between nearby letters in the plaintext. However, if ℓ is the real length, then $i\ell$ will give many coincidences for each $i = 1, 2, \ldots$. Therefore, many coincidences for displacement 2, say, but few for 4, will mean that the length is probably not 2.)
Once you have the keyword length ℓ, do frequency analysis on the ciphertext letters $y_j, y_{\ell+j}, y_{2\ell+j}, \ldots$ to find the shift there, for each $j = 1, 2, \ldots, \ell$. Combine these shifts to get the keyword.

Problem 3. (8+3 points)

(a) The plaintext *fool* is encrypted with a 2×2 Hill cipher, resulting in the ciphertext *WISE*. What is the encryption matrix? **(b)** Is it wise to use this matrix for encryption?

Solution: *fool* is (5 14 14 11), *WISE* is (22 8 18 4). If the encryption matrix is M, then

$$\begin{pmatrix} 5 & 14 \\ 14 & 11 \end{pmatrix} \cdot M = \begin{pmatrix} 22 & 8 \\ 18 & 4 \end{pmatrix} \pmod{26},$$

so we want to multiply both sides from the left with

$$\begin{pmatrix} 5 & 14 \\ 14 & 11 \end{pmatrix}^{-1} = \frac{1}{5\cdot 11 - 14\cdot 14} \begin{pmatrix} 11 & -14 \\ -14 & 5 \end{pmatrix} = \begin{pmatrix} 25 & 6 \\ 6 & 9 \end{pmatrix} \pmod{26},$$

where $1/(55-196) = 1/(-141) \equiv 1/15 \equiv 7 \pmod{26}$ was computed by the extended Euclidean algorithm:

$$\begin{aligned} 26 &= 1\cdot 15 + 11 \\ 15 &= 1\cdot 11 + 4 \\ 11 &= 2\cdot 4 + 3 \\ 4 &= 1\cdot 3 + 1 \\ 3 &= 3\cdot 1 + 0\,, \end{aligned}$$

so gcd(26,15)=1, which is not a surprise, but we can now work out the coefficients in $26x + 15y = 1$:

$$\begin{aligned} 11 &= 26 - 15 \\ 4 &= 15 - 11 = 15 - (26-15) = 2\cdot 15 - 26 \\ 3 &= 11 - 2\cdot 4 = (26-15) - 2\cdot(2\cdot 15 - 26) = 3\cdot 26 - 5\cdot 15 \\ 1 &= 4 - 3 = (2\cdot 15 - 26) - (3\cdot 26 - 5\cdot 15) = 7\cdot 15 - 4\cdot 26\,, \qquad \text{hence } y = 7\,. \end{aligned}$$

Finally,

$$M = \begin{pmatrix} 25 & 6 \\ 6 & 9 \end{pmatrix} \begin{pmatrix} 22 & 8 \\ 18 & 4 \end{pmatrix} \equiv \begin{pmatrix} 8 & 16 \\ 8 & 6 \end{pmatrix} \pmod{26}.$$

(b) The trouble with this matrix is that gcd(det(M),26)=2, hence it doesn't have an inverse (mod 26), so there's no decryption matrix. In fact, each ciphertext has many possible different plaintext sources, so proper decryption is impossible.

Problem 4. (7 points)

Assume that the 9-round Simplified DES, using the key K, encrypts the plaintext P into the ciphertext C. Show that, with the key $K \oplus 11\cdots1$, it encrypts the plaintext $P \oplus 11\cdots1$ into the ciphertext $C \oplus 11\cdots1$. (As usual, $\oplus$ means bitwise addition mod 2. And a hint: you don't need to know the expansion function and the S-boxes.)

Solution: Follow how a Feistel system works. If $P = L_0 \,||\, R_0$ and we input $P^* = P \oplus 11\cdots1$ with 9-bit key $K^* = K \oplus 11\cdots1$, then:

- the 8-bit key in each round is $K_i^* = K_i \oplus 11\cdots1$,
- $L_1^* = R_0^* = R_0 \oplus 11\cdots1$,
- $R_1^* = L_0^* \oplus f(R_0^*, K_1^*) = L_0 \oplus 11\cdots1 \oplus f(R_0 \oplus 11\cdots1, K_1 \oplus 11\cdots1)$.

So, if we prove $f(R_0 \oplus 11\cdots1, K_1 \oplus 11\cdots1) = f(R_0, K_1)$, then we get that the result of the 1st round is (the same as before)$\oplus 11\cdots1$, and then inductively this will hold in all the rounds, and we will be done.

Thus, look at

$$f(R_0 \oplus 11\cdots1, K_1 \oplus 11\cdots1) = S\big(E(R_0 \oplus 11\cdots1) \oplus (K_1 \oplus 11\cdots1)\big),$$

where $E(\cdot)$ is the expansion function, and $S(\cdot) = S_1(\cdot_{\text{left}}) \,||\, S_2(\cdot_{\text{right}})$ is the operation of the two S-boxes. Since $E(\cdot)$ is bitwise copying (just some of the bits are copied twice), we clearly have $E(R_0 \oplus 11\cdots1) = E(R_0) \oplus 11\cdots1$. Therefore, the right hand side of the displayed line equals $S\big(E(R_0) \oplus 11\cdots1 \oplus K_1 \oplus 11\cdots1\big) = S\big(E(R_0) \oplus K_1\big) = f(R_0, K_1)$, regardless of what S is, as we wanted.

Problem 5. (2+2+4 points)

(a) Define Euler's ϕ function.

Solution: $\phi(n)$ is the number of positive integers k that are less than n and relatively prime to it. E.g., $\phi(6) = 2$.

(b) State the Euler-Fermat theorem.

Solution: If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(c) Compute $1201^{1201} \pmod{707}$.

Solution: Note that $707 = 7 \cdot 101$, product of two primes, hence $\phi(707) = 6 \cdot 100 = 600$. Since gcd(1201,707)=1, Euler's theorem gives $1201^{600} \equiv 1 \pmod{707}$, thus $1201^{1201} \equiv 1201^1 \equiv 494 \pmod{707}$.

Problem 6. (5 points)

The encryption exponents $e = 1$ and $e = 2$ should not be used in RSA. Why?

Solution: If $e = 1$, then the ciphertext is $c = m^e = m$, hence there is no encryption, anyone can just read it.
If $e = 2$, and $n = pq$ with two large primes, as usually, then $\phi(n) = (p-1)(q-1)$ is even, hence we would have $\gcd(e, \phi(n)) = 2$. So there would be no decryption exponent d with $ed \equiv 1 \pmod{\phi(n)}$.