

Cryptography Assignment 2 is compulsory, and contributes 5% towards your final assessment. It should be submitted by 14:50 on Tuesday 7th April 2009. In the absence of exceptional circumstances (such as documented illness), assignments submitted after 14:50 but within 1 hour of that time will receive at most half marks, and assignments more than 1 hour late will not be marked. Make sure your name and student number are written on your submission!

Note that one of the questions on this assignment differs from student to student. You should use the same unique number as you had for the Vigenere question on the first assignment. If you have forgotten this number, contact Barbara. **Make sure you write this number clearly at the top of the first page of your assignment.**

1. (8 marks) Consider the cryptosystem with plaintext space $\mathcal{P} = \{a, b, c\}$, key space $\mathcal{K} = \{K_1, K_2, K_3\}$ and ciphertext space $\mathcal{C} = \{A, B, C\}$. The probability distributions $p_{\mathcal{P}}$ and $p_{\mathcal{K}}$ are as follows:

$$p_{\mathcal{P}}(a) = \frac{3}{8} \quad p_{\mathcal{P}}(b) = \frac{1}{8} \quad p_{\mathcal{P}}(c) = \frac{1}{2} \quad p_{\mathcal{K}}(K_1) = \frac{1}{3} \quad p_{\mathcal{K}}(K_2) = \frac{1}{2} \quad p_{\mathcal{K}}(K_3) = \frac{1}{6}$$

The encryption rules are given in the following table.

	<i>a</i>	<i>b</i>	<i>c</i>
<i>K</i> ₁	<i>A</i>	<i>B</i>	<i>C</i>
<i>K</i> ₂	<i>B</i>	<i>C</i>	<i>A</i>
<i>K</i> ₃	<i>C</i>	<i>A</i>	<i>B</i>

- (a) Determine the probability distribution of the ciphertext space, $p_{\mathcal{C}}$.
- (b) Determine whether or not this cryptosystem has perfect secrecy. Explain your answer.
2. (8 marks) An 8-bit plaintext was encrypted using a 3-stage Feistel cipher (as depicted in Exercise 5.5 of your notes) with an initial key $K = (124)(3)$ and in which each subkey k_i is the permutation obtained by applying the initial key permutation i times. The ciphertext is 10011110. Determine the plaintext. (Show all your working.)
3. (6 marks) Explain why the key 1FE01FE00EF10EF1 would be a poor choice to encrypt a message using DES.
4. (10 marks) For this question we are working in the finite field $\text{GF}(256)$ in which multiplication is carried out modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.
- (a) Determine the bitstring and polynomial representations of the field elements (in hex) $\{42\}$ and $\{a3\}$.
- (b) Determine $\{42\} \oplus \{a3\}$ giving your answer as a 2-digit hex number.
- (c) Determine the product $\{42\} \cdot \{a3\}$ using polynomial multiplication, giving your answer in polynomial form.
- (d) Determine the product $\{42\} \cdot \{a3\}$ using Tables 2 and 3 from the paper *A Specification for Rijndael, the AES Algorithm*, giving your answer as a 2-digit hex number.
- (e) Determine the inverse of $\{42\}$ using Tables 2 and 3 from the paper *A Specification for Rijndael, the AES Algorithm*, giving your answer as a 2-digit hex number.

(Please turn over.)

5. (8 marks) Below is a collection of keys for the RSA cipher. You should use the values of p , q , b and M for the line that corresponds to your file number from the first assignment.

(a) Determine the decryption exponent a , and hence find the public and private keys for this user.

(b) Find the encryption C of the message M .

(c) Use the Chinese Remainder Theorem (as outlined in lectures) to decrypt C , verifying that the answer is M .

File 1	$p = 7$	$q = 13$	$b = 11$	$M = 8$
File 2	$p = 5$	$q = 13$	$b = 7$	$M = 13$
File 3	$p = 13$	$q = 5$	$b = 7$	$M = 6$
File 4	$p = 11$	$q = 13$	$b = 13$	$M = 5$
File 5	$p = 5$	$q = 11$	$b = 13$	$M = 14$
File 6	$p = 17$	$q = 5$	$b = 7$	$M = 15$
File 7	$p = 13$	$q = 7$	$b = 7$	$M = 11$
File 8	$p = 17$	$q = 13$	$b = 11$	$M = 14$
File 9	$p = 13$	$q = 11$	$b = 13$	$M = 9$
File 10	$p = 7$	$q = 11$	$b = 7$	$M = 8$
File 11	$p = 17$	$q = 11$	$b = 9$	$M = 10$
File 12	$p = 5$	$q = 13$	$b = 11$	$M = 11$
File 13	$p = 7$	$q = 13$	$b = 7$	$M = 6$
File 14	$p = 5$	$q = 13$	$b = 11$	$M = 7$
File 15	$p = 17$	$q = 11$	$b = 9$	$M = 13$
File 16	$p = 11$	$q = 7$	$b = 7$	$M = 14$
File 17	$p = 17$	$q = 5$	$b = 9$	$M = 7$
File 18	$p = 17$	$q = 13$	$b = 7$	$M = 14$
File 19	$p = 13$	$q = 11$	$b = 7$	$M = 9$
File 20	$p = 7$	$q = 11$	$b = 7$	$M = 8$
File 21	$p = 11$	$q = 7$	$b = 13$	$M = 7$
File 22	$p = 17$	$q = 7$	$b = 11$	$M = 9$
File 23	$p = 7$	$q = 13$	$b = 7$	$M = 8$
File 24	$p = 13$	$q = 7$	$b = 7$	$M = 6$
File 25	$p = 5$	$q = 13$	$b = 11$	$M = 12$
File 26	$p = 11$	$q = 13$	$b = 11$	$M = 9$
File 27	$p = 17$	$q = 11$	$b = 13$	$M = 15$
File 28	$p = 13$	$q = 11$	$b = 7$	$M = 8$
File 29	$p = 17$	$q = 5$	$b = 9$	$M = 14$
File 30	$p = 13$	$q = 11$	$b = 13$	$M = 8$
File 31	$p = 5$	$q = 11$	$b = 13$	$M = 15$
File 32	$p = 11$	$q = 13$	$b = 7$	$M = 11$
File 33	$p = 13$	$q = 11$	$b = 11$	$M = 6$
File 34	$p = 13$	$q = 11$	$b = 13$	$M = 7$
File 35	$p = 17$	$q = 13$	$b = 13$	$M = 12$
File 36	$p = 17$	$q = 5$	$b = 9$	$M = 5$
File 37	$p = 5$	$q = 11$	$b = 11$	$M = 7$
File 38	$p = 5$	$q = 11$	$b = 7$	$M = 13$
File 39	$p = 17$	$q = 13$	$b = 11$	$M = 13$
File 40	$p = 11$	$q = 5$	$b = 11$	$M = 7$
File 41	$p = 5$	$q = 11$	$b = 7$	$M = 15$
File 42	$p = 17$	$q = 5$	$b = 7$	$M = 14$
File 43	$p = 5$	$q = 11$	$b = 9$	$M = 9$
File 44	$p = 17$	$q = 7$	$b = 7$	$M = 14$
File 45	$p = 5$	$q = 11$	$b = 9$	$M = 14$
File 46	$p = 17$	$q = 7$	$b = 11$	$M = 9$
File 47	$p = 5$	$q = 11$	$b = 7$	$M = 8$
File 48	$p = 17$	$q = 7$	$b = 11$	$M = 15$