CS547A 2003 Homework set #2

Due Friday October, 10 2003 in class at 13:30 SHARP

Exercise from Stinson's book (second edition) 1.21 (1.1 former editions)

Exercises

A. Consider the following two sets of hash functions on **m** bit inputs:

H_0 = **{ h(x) = (Mx)⊕y | M** is an **mxm** binary matrix and **y** is an **m** bits string }
H_1 = **{ h(x) = (Mx)⊕y | M** is an **mxm** binary invertible matrix and **y** is an **m** bits string }

For each of these two sets prove whether or not they are Strongly Universal$_2$ classes of hash functions. Here, the product **z** of a matrix **M** with a bit vector **v** is done by apply the □ (AND) operation bitwise and then the ⊕ (XOR) operation on the results.

$$z_j = \bigoplus_i \, (M_{ij} \,\square\, v_i)$$

For example (10010) [010] = (0⊕0⊕0⊕1⊕0 , 1⊕0⊕0⊕0⊕0, 0⊕0⊕0⊕0⊕0) = (110).
[111]
[001]
[100]
[101]

B. **MAPLE**

AUTHENTICATION CODES and finite fields

You are now asked to setup an authentication code over $\mathbf{F}_2$1000.

1. Using **MAPLE™** find a random irreducible polynomial **P** of degree **1000** over $\mathbf{F}_2$.
WARNING: do not use MAPLE functions Randprime and Randpoly !!!
Suggestion: Generate your own random polynomials...
For extra bonus credits: explain the source of the problem with Randpoly.

2. Build the field $\mathbf{F}_2$1000 with the irreducible polynomial **P** found above.

3. Find a primitive element **g** of $\mathbf{F}_2$1000.

4. Pick two random elements **(i,j)** in $\mathbf{F}_2$1000.

5. Tell us **x,y, 0<= x,y < 2^{1000}-1** such that **g^x=i** and **g^y=j**.

... more on back

6. Pick a message **m** of **1000** bits that you like and calculate the corresponding tag **t** made of the **50** least significant bits (the coefficients of the terms of degree less than **50**) of **m*i+j** over $\mathbf{F}_{2^{1000}}$. (<u>no credit question:</u> tell us why you like **m**.)

7. Send us **(P,i,j)** and **(m,t)** via e-mail to gsavvi1@cs.mcgill.ca before this HW deadline.

Useful info:

$2^{1000}-1 = (2^{500}-1)*(2^{500}+1)$
$2^{500}-1 = (2^{250}-1)*(2^{250}+1)$
$2^{250}-1 = (2^{125}-1)*(2^{125}+1)$
$2^{250}+1 = (2^{125}-2^{63}+1)*(2^{125}+2^{63}+1)$
$2^{500}+1 = (2^{100}+1)*(2^{400}-2^{300}+2^{200}-2^{100}+1)$

$2^{125}-1 = 31 * 601 * 4710883168879506001 * 269089806001 * 1801$
$2^{125}+1 = 3 * 11 * 251 * 229668251 * 5519485418336288303251 * 4051$
$2^{125}-2^{63}+1 = 5^4 * 94291866932171243501 * 268501 * 28001 * 96001$
$2^{125}+2^{63}+1 = 41 * 101 * 47970133603445383501 * 3775501 * 7001 * 8101$
$2^{100}+1 = 17 * 61681 * 401 * 3173389601 * 2787601 * 340801$
$2^{400}-2^{300}+2^{200}-2^{100}+1 = 4001 * 1074001 * 2020001 * 22624001 * 1481124532001$

<u>HILL CIPHER</u>

Extend the alphabet used in the Hill cipher with three new symbols: " " (spacebar), "." (dot), "," (comma) to improve readability of texts. We encode these new symbols numerically as **26 (" ")**, **27 (".")**, **28 (",")**. We now consider the Hill cipher with an alphabet of **29** symbols (instead of **26**) and thus perform all operation **mod 29**.

8. Using **MAPLE™** decrypt the following ciphertext **c** encrypted with matrix **K**

```
        [1, 2, 3, 4]
K : =   [2, 3, 4, 0]
        [3, 4, 0, 0]
        [4, 0, 0, 0]
c: = 23 06 26 08 12 10 26 18 20 21 13 14 22 04 27 18 25 07 06 24 21 20 16 18 17 08 02 23
```

9. Using **MAPLE™** find the number of invertible **2x2** matrices over $\mathbf{F}_{29}$.
(use without proof the following claim: **[M** is not invertible iff **det(M)=0]** over $\mathbf{F}_q$)

10. Give an expression for the number of invertible **nxn** matrices of $\mathbf{F}_{29}$.
<u>Hint</u>: Stinson's book, exercise 1.12

11. Using **MAPLE™** find a counter-example to the above claim over $\mathbf{Z}_{26}$**:**
A **2x2** matrix **M** which is not invertible over $\mathbf{Z}_{26}$ but such that **det(M)>0** over $\mathbf{Z}_{26}$.

12. Using **MAPLE™** find the number of invertible **2x2** matrices over $\mathbf{Z}_{26}$.
<u>Hint :</u> read page 16 of Stinson's book.

13. In the light of the above questions, explain why I changed the alphabet size to **29**?

... more on back