CS547A 2003 Homework set #3

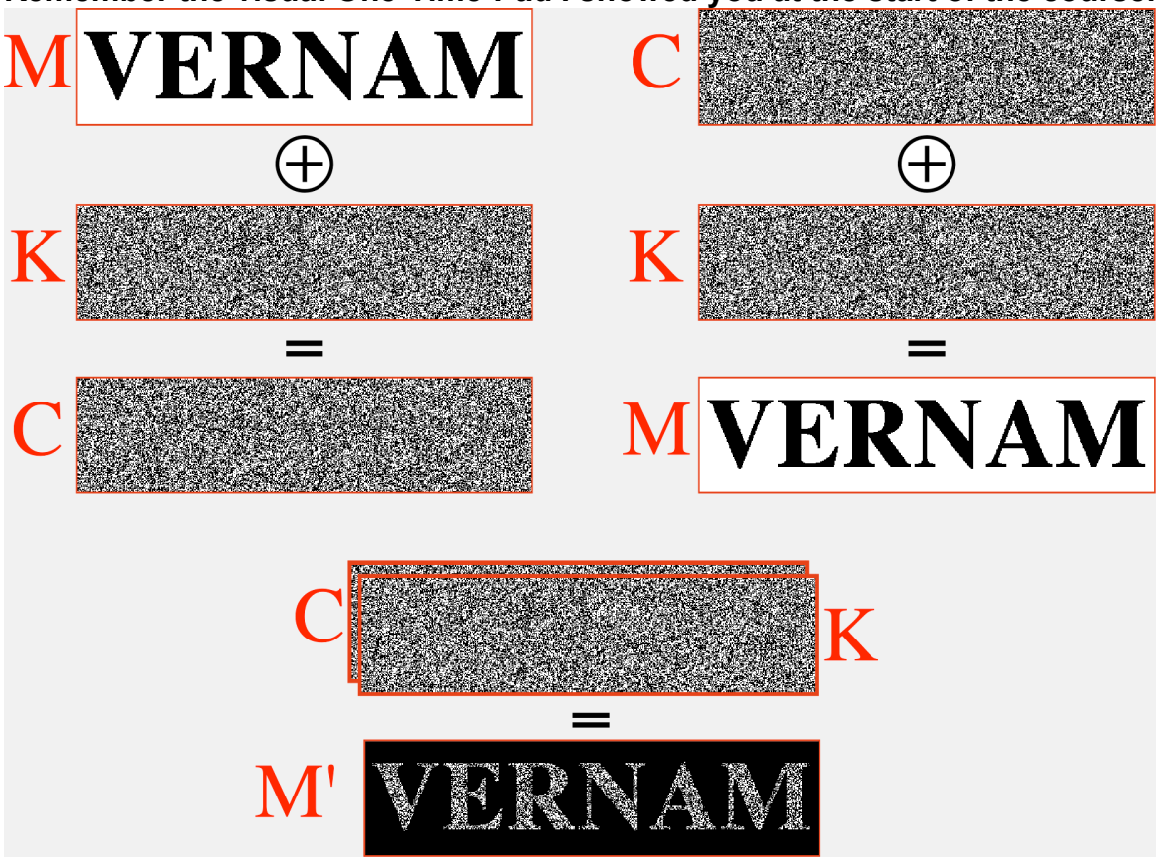
Due Monday October, 27 2003 in class at 13:30 SHARP

Exercises (from Stinson's book) • 4 questions •

Information theory: Ex 2.2, 2.5, 2.13, 2.15 (formerly 2.1, 2.4, 2.10, 2.12)

Exercises (home-made) • 4 questions •

Remember the visual One-Time-Pad I showed you at the start of the course.



A) Explain why superposition of K and C produces a readable image M' of the plaintext M, although in reality M should be obtained by C XOR K.

B) Explain the importance of redundancy in the plaintext, and what would happen if the plaintext contained none.

...more on back

Consider the variation on the Blum-Blum and Shub generator (mod N=pq) where we output L blocks of all the bits computed in each iteration :

BBS*(s_0)
L:=length/|N|
FOR i:=1 TO L DO $s_i := (s_{i-1})^2 \bmod N$
RETURN s_1 || s_2 || ... || s_L

C) Show how to distinguish the output of BBS* from a truly random source, even without knowing N nor its length |N|.

D) Write a Maple™ program to implement your distinguisher and run it on the examples below. Find which of W_0 and W_1 is generated by BBS*.

W_0=

0010001011001110011010101101111111101101100001100001011110110110000101
0110100001100101111111110100101111010011010011110011001101001100111101
1010100100100111010011000000101111101000000110011010111000000110110010
0010100101111010111110101001110011000011101101101010111100010101100101
1001010011000010100000111010011110000110000100001011110110001000001100
1010100011100011101011001001010100111010000011110110011010110111101110
1111010111001000100011110001100100010111100001101100010011111000101111
0100000010101010011111101100101010101100101010000010110111110010000011
1111001101001011101101011011011100001010111010000011010010000000110001
0010110010001101001000001101100100110010100100100001110011101011000010
1111101101110011110010110011001110001111110001001110010101111100001010
0100000100001001110100001011100011010000011000110110001010110011110111
0100010010100001000101101001000010110110100111011100100110011010100100
1110110111011100000010000011101110000111111010101010001100100011101000
0000000101111010001100000011110110101101111101110110000011000010010111
1101111101001000011100100100111011010011001001000011110010000100000010
1001100011010010010110111001101010110001111101111000101010110000111 0

W_1=

0100101001101000001100011100001101100011111110011001011100111110101111
0000011010000000101101011111011100000000110110011001000011100011001101
0010110101101100000101100111110101010110010101111110101010001010110011
0101111000010001110011010001000111000000100100001010001011110100100111
1010101110011101000010110101111100101010001111000111100110010111110111
0100001000001100010111100110010010101001110101111110010010011111101111
0111010011000000110111001101011101000101011011101010111000100000100111
1011100100010010001010111011000010101001100101000110110011001001111111
0100011000100010000000111110001101001100011000010101001001011001100010
0010010001000010101001100110010001111110110010000000111110000110101011
0011011000011010011101010101111100001110100001011110010001001001110100
1010010100111000011101111110101011000111101000011001111000100101111000
1101011110111111011110010111001101100100011101101010010100000000101001
1101000000000101111000000100111000110001010000000110011111010101111000
0110011101100110100010011011011111101101100101001011011101101101010100
1111110000110100110001000110111111110111110111111010010000001111110101
0010101100100101101100000001001110001110010001101101010010011101010 1