Solutions to final exam in CRYPTOGRAPHY on 15 December 2004.

Problem 1:
(a) This corresponds to a simple substitution cipher. The number of different keys is $|K| = 26!$. Then

$$N_0 = \frac{H(K)}{D} = \frac{\log 26!}{3.2} \approx 28,$$

assuming $D = 3.2$ for English text.

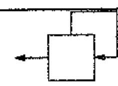
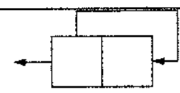
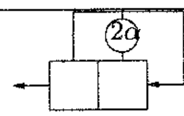
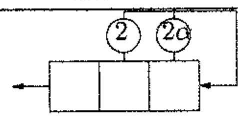
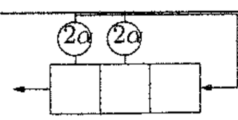
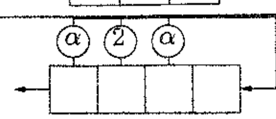
(b) A simple substitution cipher contains all different permutations on $\mathbf{Z}_{26}$. If we concatenate a substitution cipher with fixed key K and Caesar cipher with the key K, the result is still a permutation on $\mathbf{Z}_{26}$. The number of nonequivalent keys does not increase and $N_0 = 28$ as in (a).

(c) The given system cannot increase N_0 by double encryption or something similar (it is not possible to increase $H(K)$). Instead, we must decrease D. This can be done by either *source compression* or *homophonic coding.*

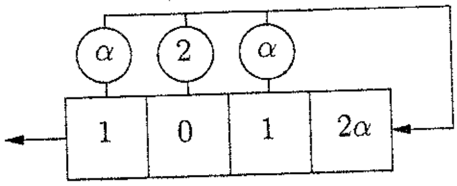
Problem 2:
(a) The sequence is $s = (1, 0, 1, 2\alpha, 2\alpha, \alpha+1, 2)$ over $\mathbf{F}_{3^2}$ with $p(x) = x^2 + x + 2$. First let us make a table of elements in this field:

$\alpha^1 = \alpha$	$\alpha^5 = 2\alpha$
$\alpha^2 = 2\alpha + 1$	$\alpha^6 = \alpha + 2$
$\alpha^3 = 2\alpha + 2$	$\alpha^7 = \alpha + 1$
$\alpha^4 = 2$	$\alpha^8 = 1$

To find the shortest linear feedback shift register we use Berlekamp-Massey's algorithm:

S_N	d	$C_1(z)$	$C(z)$	L	Shift Register	$C_0(z)$	d_0	e	N
–	–	–	1	0	$\leftarrow$	1	1	1	0
1	1	1	$1 + 2z^{-1}$	1		1	1	1	1
0	2	$*$	1	$*$		$*$	$*$	2	2
1	1	1	$1 + 2z^{-2}$	2		1	1	1	3
2α	2α	$*$	$1 + \alpha z^{-1} + 2z^{-2}$	$*$		$*$	$*$	2	4
2α	1	$1 + \alpha z^{-1} + 2z^{-2}$	$1 + \alpha z^{-1} + z^{-2}$	3		$1 + \alpha z^{-1} + 2z^{-2}$	1	1	5
$\alpha + 1$	α	$*$	$1 + \alpha z^{-2} + \alpha z^{-3}$	$*$		$*$	$*$	2	6
2	2α	$1 + \alpha z^{-2} + \alpha z^{-3}$	$1 + 2\alpha z^{-2} + z^{-3} + 2\alpha z^{-4}$	4		$1 + \alpha z^{-2} + \alpha z^{-3}$	2α	1	7

So, the final feedback shift register is



(b) The given sequence is $s = [0,0,0,1,1]^\infty$.

$$S(z) = \frac{z^{-3}+z^{-4}}{1+z^{-5}} = \frac{z^{-3}(1+z^{-1})}{(1+z^{-1}+z^{-2}+z^{-3}+z^{-4})(1+z^{-1})} = \frac{z^{-3}}{1+z^{-1}+z^{-2}+z^{-3}+z^{-4}}.$$

Hence, the answer is $C(z) = 1+z^{-1}+z^{-2}+z^{-3}+z^{-4}$.

Problem 3:
(a) We consider the $(3,5)$ Shamir's scheme over $\mathbf{F}_{101}$

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} a_2x_1^2 + a_1x_1 + a_0 \\ a_2x_2^2 + a_1x_2 + a_0 \\ a_2x_3^2 + a_1x_3 + a_0 \end{pmatrix} \Rightarrow \left(\begin{array}{ccc|c} 1 & 1 & 1 & 40 \\ 1 & 2 & 4 & 50 \\ 1 & 3 & 9 & 60 \end{array}\right) \Rightarrow$$

$$\left(\begin{array}{ccc|c} 1 & 1 & 1 & 40 \\ 0 & 1 & 3 & 10 \\ 0 & 2 & 8 & 20 \end{array}\right) \Rightarrow \left(\begin{array}{ccc|c} 1 & 0 & -2 & 30 \\ 0 & 1 & 3 & 10 \\ 0 & 0 & 2 & 0 \end{array}\right) \Rightarrow K = a_0 = 30$$

(b) $M = (m_1, m_2)$, $K = (k_1, k_2)$, $C = (m_1, m_2, t)$ over $\mathbf{F}_3$, where $t = k_1 + m_1k_1 + m_2k_2$.

$$P_I = \max_{C} P(C \text{ valid}) = \max_{(m_1,m_2,t)} \frac{|\{(k_1,k_2) : t = k_1 + m_1k_1 + m_2k_2\}|}{|\{(k_1,k_2) : k_1, k_2 \in \mathbb{F}_3\}|} = \begin{bmatrix} \text{choose} \\ t=0 \\ m_1 = 2 \\ m_2 = 0 \end{bmatrix} = \frac{9}{9} = 1$$

$$P_S = \max_{\substack{C, C' \\ C \neq C'}} P(C' \text{ valid} \mid C \text{ valid}) = \max \frac{\left|\left\{(k_1,k_2) : \begin{matrix} t = k_1 + m_1k_1 + m_2k_2 \\ t' = k_1 + m_1'k_1 + m_2'k_2 \end{matrix}\right\}\right|}{|\{(k_1,k_2) : t = k_1 + m_1k_1 + m_2k_2\}|} = \begin{bmatrix} m_1 = m_2 = t = 0 \\ m_1' = 1, m_2' = 0 \\ t' = 0 \end{bmatrix} = \frac{3}{3} = 1$$

Problem 4:
We need to factorize the number $n = 44384521$.

$$1883840^2 \equiv 3 \mod n$$
$$6521874^2 \equiv 2 \cdot 3 \cdot 5 \mod n$$
$$13519124^2 \equiv 13 \mod n$$
$$16006155^2 \equiv 2 \cdot 5 \mod n$$

We calculate X and Y as follows

$$\begin{cases} X = 1883840 \cdot 6521874 \cdot 16006155 \equiv 37147551 \mod n \\ Y = 2^1 \cdot 3^1 \cdot 5^1 \equiv 30 \mod n \end{cases}$$

Then we have $X^2 \equiv Y^2 \mod n$. If $n = p \cdot q$, then one of the factors could be ~~is~~:

$$p = \gcd(44384521, 37147551 + 30) \Rightarrow$$

$$\begin{aligned}
44384521 &= 1 \cdot 37147581 + 7236940 \\
37147581 &= 5 \cdot 7236940 + 962881 \\
7236940 &= 7 \cdot 962881 + 496773 \\
962881 &= 1 \cdot 496773 + 466108 \\
496773 &= 1 \cdot 466108 + 30665 \\
466108 &= 15 \cdot 30665 + 6133 \\
30665 &= 5 \cdot 6133 \\
&\Rightarrow p = 6133; q = \frac{n}{p} = 7237
\end{aligned}$$

Problem 5: $p(x) = 1 + x^2 + x^3 + x^4 + x^5$, $p(\alpha) = 0$.

3

(a) If $p(x)$ over $\mathbf{F}_2$ is irreducible?

$$\begin{cases} p(0) = 1 \\ p(1) = 1 \end{cases} \Rightarrow \quad \text{No factors of degree 1.}$$

Check if $x^2+x+1 \mid x^5+x^4+x^3+x^2+1$ by long division. No! $\Rightarrow p(x)$ irreducible.

(b) We need to check the order of the element α in the extention field $\mathbf{F}_{2^5}$. By Lagrange theorem the order of any element from this field must divide $2^5 - 1 = 31$. Since 31 is a prime number, and order(α)$\neq 1$, then order(α) must be 31, i.e., $p(x)$ is a primitive polynomial.

(c) We need to find the cycle set of $p(x)$ over $\mathbf{F}_3$.

(1) Factorization of $p(x)$ over $\mathbf{F}_3$.

$$\begin{cases} p(0) = 1 \\ p(1) = 5 \quad 2 \\ p(2) = 1 + 4 + 8 + 16 + 32 = 61 \quad 1 \end{cases} \Rightarrow \quad \text{No factors of degree 1.}$$

Check for factors of degree 2: $p(x) = (x^3 + ax^2 + bx + c)(x^2 + dx + e)$

$$\begin{cases} c\cdot e = 1 \\ c\cdot d + b\cdot e = 0 \\ c + b\cdot d + a = 1 \\ b + a\cdot d + e = 1 \\ a + d = 1 \end{cases} \Rightarrow$$

Assume $c = e = 1$

$$\begin{cases} d + b = 0 \\ b\cdot d + a = 0 \\ b + a\cdot d = 0 \\ a + d = 1 \end{cases}$$

$\Rightarrow$ no solutions!

Assume $c = e = 2$

$$\begin{cases} d + b = 0 \\ b\cdot d + a = 2 \\ b + a\cdot d = 2 \\ a + d = 1 \end{cases}$$

$\Rightarrow$ The solution is $(a, b, c, d, e) = (0, 2, 2, 1, 2)$

Hence, the polynomial is factorized as $p(x) = (x^3 + 2x + 2)(x^2 + x + 2)$. None of the factors can be factorized again since $p(x)$ has no factors of degree 1, as shown in the previous step.

(2) Consider $a(\alpha) = \alpha^3 + 2\alpha + 2 = 0$ (i.e., $\alpha^3 = \alpha + 1$) as a generating polynomial for $\mathbf{F}_{3^3}$. To construct a cycle set for $a(\alpha)$ we need to find the period T_a =order(α). The extension field has $3^3 = 27$ elements, i.e., the order(α) can only be one of $\{1, 2, 13, 26\}$.

$$\begin{aligned}
\alpha^1 &= \alpha \neq 1 \\
\alpha^2 &= \alpha^2 \neq 1 \\
\alpha^4 &= \alpha\cdot\alpha^3 = \alpha^2 + \alpha \\
\alpha^8 &= (\alpha^4)^2 = 2\alpha^2 + 2 \\
\alpha^{12} &= \alpha^4\cdot\alpha^8 = (\alpha^2+\alpha)(2\alpha^2+\alpha) = \alpha^2 + 2 \\
\alpha^{13} &= \alpha\cdot\alpha^{12} = \alpha\cdot(\alpha^2+2) = 1(!) .
\end{aligned}$$

Hence, T_a =order(α)=13, and the cycle set is $1(1) \oplus \frac{3^3-1}{13}(13)$.

(3) Consider $b(x) = x^2 + x + 2$, $C(z) = \frac{b(z)}{z^2} = 1 + z^{-1} + 2z^{-2}$. We can find the period T_b via long division as follows.

```
    1  0  0| 1  1  2
  - 1  1  2| 1  2  2  0  2  1  1  0
    -------
       2  1
   -   2  2  1
       -------
          2  2
      -   2  2  1
          -------
             2
         -   2  2  1
             -------
                1  2
            -   1  1  2
                -------
                   1  1
               -   1  1  2
                   -------
                         1
```

$\Rightarrow T = 8 \quad \Rightarrow 1(1) \oplus 1(8)$

(4) Multiplication of cycle sets:

$$(1(1) \oplus 2(13)) \otimes (1(1) \oplus 1(8)) = 1(1) \oplus 1(8) \oplus 2(13) \oplus 2(104)$$

(5) Check the sum: $3^5 = 243$; $1\cdot 1 + 1\cdot 8 + 2\cdot 13 + 2\cdot 104 = 243$