MATH/CMSC 456 FINAL EXAM
ANSWERS SPRING 2003

1. (a) Vigenère: plaintext=*aaaaaaaa*.... The ciphertext will be the key, repeated several times.
(b) Hill: plaintext=*baab*. This becomes the vectors $(1,0)$ and $(0,1)$. Multiplying $(1,0)$ times the matrix gives the first row of the matrix. Multiplying $(0,1)$ times the matrix gives the second row of the matrix.
(c) Affine: plaintext=*ab*. If the encryption function is $mx+n$, then $a=0$ encrypts to the value of n, so we obtain n. Also, $b=1$ encrypts to $m+n$, so we can subtract n and obtain m.

2. (a) Solve $3d \equiv 1 \pmod{40}$, since $(5-1)(11-1)=40$. The solution is $d=27$.
(b) $c^{27} \equiv (m^3)^{27} \equiv m^{81} \equiv (m^{40})^2 m \equiv 1^2 m \equiv m \pmod{55}$. This uses Euler's theorem: $m^{40} \equiv 1 \pmod{55}$.

3. (a) gcd(670705093 − 33335, 670726081) is a nontrivial factor.
(b) The sequence starts $1,0,1,0,1,\ldots$. Assume $k_{n+2} = c_0 k_n + c_1 k_{n+1}$. Then

$$k_3 \equiv 1 \cdot c_0 + 0 \cdot c_1, \qquad k_4 \equiv 0 \cdot c_0 + 1 \cdot c_1.$$

This yields $c_0 = 1, c_1 = 0$, so the recurrence is $k_{n+2} = k_n$.

4. (a) Alice needs to solve $s_1^e \equiv m_1 \pmod{n}$. This is the same as decrypting the RSA "ciphertext" m_1 to obtain the "plaintext" s_1. This should be hard if RSA is secure.
(b) We automatically have $m_2 \equiv s_2^e$, so the signature is valid.
(c) Eve needs to find m_3 with $H(m_3) \equiv s_3^e \pmod{n}$. Since H is preimage resistant, this should be hard.

5. After one round: Left=M_1, Right=$M_2 = M_1 \oplus K \oplus M_0$.
After 2 rounds: Left=$M_2 = M_0 \oplus M_1 \oplus K$, Right=$M_3 = M_2 \oplus M_1 \oplus K = M_0$.
After 3 rounds: Left=$M_3 = M_0$, Right=$M_2 \oplus K \oplus M_3 = M_1$.
(a) After 2 rounds, you know M_0 and you know $M_0 \oplus M_1 \oplus K$, so you know $M_1 \oplus K$. But you can't separate M_1 and K, so you cannot deduce K.
(b) After 3 rounds, you have the original plaintext, so the system is not secure.

6. Peggy chooses r_1, r_2 as described and sends the values of x_1, x_2 to Victor, who checks that $x_1 x_2 \equiv \beta$. Then Victor asks Peggy for either r_1 or r_2. Peggy sends that r_i and Victor checks that $x_i \equiv \alpha^{r_i} \pmod{p}$. This is repeated at least 10 times (since $1/2^{10} < 1/1000$).

7. (a) The line through B and C has slope $(8-3)/(3-2) = 5$. The equation of the line is $y = 5x + 6$. The secret is 6.
(b) The slope of the line through B and D is $(7-3)/(4-2) = 2$. This is not the line from part (a), so D cannot have a valid share.

8. (a) $aB = abQ = baQ = bA$.
(b) Eve knows Q and $A = aQ$, so she finds a by computing discrete logs. She then computes aB and extracts the key.
(c) p is a prime and α is a primitive root mod p. Alice and Bob choose secret a and b. Alice computes $A \equiv \alpha^a \pmod{p}$ and Bob computes $B \equiv \alpha^b \pmod{p}$. Alice sends A to Bob and Bob sends B to Alice. Alice computes $B^a \pmod{p}$ and Bob computes $A^b \pmod{p}$. They extract the last 100 bits of these (equal) numbers to obtain their key.