MATH/CMSC 456 (Washington) Exam 1 SOLUTIONS March 21, 2003

1. (a) If $y \equiv \alpha x + \beta$, then $x \equiv \alpha^{-1}(x - \beta)$. To decrypt, you need $\gcd(\alpha, 30) = 1$. The possible values of α are 1, 7, 11, 13, 17, 19, 23, 29.
(b) We need two numbers x_1, x_2 with $10x_1 \equiv 10x_2 \pmod{30}$. One example is $x_1 = 0, x_2 = 3$. The plaintext letters are a and d.

2. (a) shift cipher: They ciphertext consists of the key repeated many times, so Eve can determine the key.
(b) affine cipher: If the encryption function is $\alpha x + \beta$, then $a = 0$ encrypts to β. Therefore the ciphertext consists of the letter corresponding to β, repeated many times. Eve cannot find out the key because she cannot determine α.
(c) Hill cipher, with a 2×2 matrix: The plaintext $aaaa\ldots$ corresponds to several 0 vectors. These encrypt to 0 vectors. This does not depend on the matrix, so Eve obtains no information about the matrix.
(d) Vigenère cipher: The ciphertext consists of the key repeated several times. Eve therefore finds the key.

3. The matrix equation is

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}.$$

4. (15 points) Eve finds d with $ed \equiv 1 \pmod{12345}$. Then $ed = 1 + 12345k$ for some k, so

$$c^d \equiv m^{ed} \equiv m^{1+12345k} \equiv m(m^{12345})^k \equiv m(1)^k \equiv m \pmod{n}.$$

5. (13 points) Use the Chinese Remainder Theorem to solve

$$x \equiv 7 \pmod{p}, \qquad x \equiv -7 \pmod{q}.$$

Then $x^2 \equiv 49 \pmod{p}$ and $\pmod{q}$, hence $\pmod{pq}$. But $x \not\equiv \pm 7 \pmod{pq}$.

6. (a) If $k^2 \not\equiv 1 \pmod{n}$, then $2^{n-1} \equiv k^2 \not\equiv 1 \pmod{n}$. Fermat's theorem implies that n cannot be prime.
(b) We have $k^2 \equiv 1^2 \pmod{n}$ but $k \not\equiv \pm 1 \pmod{n}$. Therefore $\gcd(k-1, n)$ is a nontrivial factor of n.