1. (a) The cipher $(12, 3, 6, 19, 10)$ was encrypted by an affine cipher modulo 20. The first two plaintext symbols were 7 and 4. Find the key.

Encryption was $E(x) = ax + b \pmod{20}$ for some $a, b$. Thus we have $7a + b \equiv 12 \pmod{20}$ and $4a + b \equiv 3 \pmod{20}$. Subtracting gives $3a \equiv 9 \pmod{20}$, so $a \equiv 3 \pmod{20}$. Then the second equation gives $4 \cdot 3 + b \equiv 3 \pmod{20}$, so $b = 11$.

(b) Suppose we use a Hill cipher whose key is a $k \times k$ matrix $M$ modulo $n$. What constraint must we put on $M$? How many valid keys are there if $n$ is a prime?

The determinant of $M$ must be relatively prime to $n$.

There are $n^k - 1$ ways to choose the first row (any nonzero row). There are $n^k - n$ ways to choose the second row (not a multiple of the first row). There are $n^k - n^2$ ways to choose the third row (linearly independent of the first 2 rows). In general there are $n^k - n^{i-1}$ ways to choose the $i$th row (linearly independent of the first $i-1$ rows). In all there are $\prod_{i=1}^{k} (n^k - n^{i-1})$ choices for $M$.

2. (Extra credit answer is in parentheses.)

(a) How many square roots does 126 have modulo 385? Show how you got your answer.

We have $385 = 5 \cdot 7 \cdot 11$. 126 (mod 5) = 1 has two square roots (1, −1 = 4) modulo 5 trivially. 126 (mod 7) = 0 has one square root (0) modulo 5 trivially. 126 (mod 11) = 5. We have $(±4)^2 \equiv 5 \pmod{11}$ (e.c.: this can be found by searching or by computing $5^{(11+1)/4} \equiv 4 \pmod{11}$), so it has two square roots (e.c.: 4,7) modulo 11.

This gives 4 combined choices of square roots of 126 mod 5, 7, and 11 (e.c.: (1,0,4), (1,0,7), (4,0,4), (4,0,7)). So there is a total of 4 square roots.

(b) Explain how to find the square roots of 126 modulo 385 using the Chinese Remainder Theorem.

First run the EEA with 5 and 7 to find $a, b$ with $5a + 7b = 1$. (e.c.: We get $a = 3, b = -2$.) Then run the EEA with 35 and 11 to find $c, d$ with $35c + 11d = 1$. (e.c.: We get $c = 6, d = -19$.)

Now for each $x, y, z$, square roots of 126 mod 5, 7, and 11 do the following. Then find $w = y \cdot 5a + x \cdot 7b$, a square root of 126 mod 35, and $v = z \cdot 35c + w \cdot 11d$, a
square root of 126 modulo 385. (e.c.: This gives the square roots 301, 161, 224, 84.)

3. (a) How can the Extended Euclidean Algorithm be used to find the inverse of an integer $a$ modulo an integer $m$?

Run EEA on input $a, m$. This gives $s, t$ with $as + mt = \gcd(a, m)$. If this gcd is 1, then $a^{-1} \pmod{m} = s$.

(b) Let $a$ and $b$ be positive integers. Prove that there are integers $q, r$ so that $a = qb + r$ and $0 \leq r < b$.

By induction on $a$. Base case: If $a < b$, take $q = 0$ and $r = a$. Induction case: If $a \geq b$, then $0 \leq a - b < a$, so by induction there exist $q'$ and $r'$ so that $a - b = q'b + r'$. Then $a = (q' + 1)b + r'$, so we can take $q = q' + 1$ and $r = r'$.

Or:
Let $S = \{x = a - qb : x \geq 0\}$. $S$ is a nonempty set of natural numbers so it has a minimal element $r = a - qb$. If $r \geq b$, then $r - b \geq 0$ and $r - b = a - (q + 1)b \in S$. This contradicts the minimality of $r$, so $0 \leq r < b$ and $a = qb + r$.

4. (20 pts)

(a) Let $(R, +, \cdot, 0, 1)$ be a commutative ring. Prove that for every $a \in R$ we have $0 \cdot a = 0$.

We know that $0 + 0 = 0$. Then $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$. Adding $-(0 \cdot a)$ to both sides gives $0 = (0 \cdot a)$.

(b) Let $(F, +, \cdot, 0, 1)$ be a finite field. Define the characteristic of $F$ and show that the characteristic is prime.

The characteristic of $F$ is the unique positive generator of the kernel of the homomorphism $f$ from $\mathbb{Z}$ to $F$ defined by $f(1) = 1$. Or, it is the smallest positive integer $p$ such that adding $p$ 1s gives 0.

If the characteristic $p$ were not prime, then $p = ab$ with $a, b < p$. Then $0 = f(p) = f(a)f(b)$, but $f(a), f(b) \neq 0$. But then $0 = 0 \cdot f(b)^{-1} = f(a)f(b)f(b)^{-1} = f(a)$, which is a contradiction.

5. (a) A Feistel transformation is a function of the form

$$E_K(L_0, R_0) = (R_0, L_0 \oplus f(K, R_0)) = (L_1, R_1),$$

where $K$ is the key, $L_0, R_0, L_1, R_1$ are each $n$ bit words, and $f(K, R_0)$ is an arbitrary function from $n$ bits to $n$ bits.
Prove that every Feistel transformation is invertible. That is, show how to find $L_0$ and $R_0$ if $L_1$, $R_1$, and $K$ are known.

Given $(L_1, R_1)$, we immediately have $R_0 = L_1$. Then $R_1 = L_0 \oplus f(K, R_0) = L_0 \oplus f(K, L_1)$, so $L_0 = R_1 \oplus f(K, L_1)$. That is,

$$(L_0, R_0) = (R_1 \oplus f(K, L_1), L_1).$$

(b) Let $E_K$ denote the encryption function of a block cipher with key $K \in \{0, 1\}^n$. Suppose we try to strengthen this cipher by using two keys, $K, L \in \{0, 1\}^n$ and encrypting message $m$ by $E'_{K,L}(m) = E_K(E_L(m))$. Describe a known plaintext attack on this cryptosystem that’s faster than exhaustive search. How much faster is it, and how much memory does it use?

Meet in the middle attack: Given plaintext/ciphertext pair $(m, c)$, build lists $A = \{(E_I(m), I) : I \in \{0, 1\}^n\}$ and $B = \{(D_J(c), J) : J \in \{0, 1\}^n\}$. Then look for $(x, I) \in A, (x, J) \in B$. This can be done by sorting $A$ on first components and binary searching in $A$ for each element of $B$.

Exhaustive search takes $2^{2n+1}$ encryptions. Meet in the middle takes $2^{n+2}$ encryptions and uses $2 \cdot 2^{n+k}(n + k)$ bits of memory, where $k$ is the message length.