**31.5-1** According to Chinese Remainders theorem, the solution is to modulo 55. We find $M_1 = 5^{-1} \mod 11 = 9$ and $M_2 = 11^{-1} \mod 5 = 1$, and therefore $c_1 = 5M_1 = 45$ and $c_2 = 11M_2 = 11$. Therefore, one solution is given by $x = (5c_1 + 4c_2) \mod 55 = (5 \cdot 45 + 4 \cdot 11) \mod 55 = 49$, and the rest are of the form $55k + 49$ for $k \in \mathbb{Z}$.

**31.5-2** According to Chinese Remainders theorem, the solution is to modulo $9 \cdot 8 \cdot 7 = 504$. We find, $m_1 = 8 \cdot 7 = 56$, $m_2 = 9 \cdot 7 = 63$ and $m_3 = 9 \cdot 8 = 72$. The inverses are $M_1 = 56^{-1} \mod 9 = 2^{-1} \mod 9 = 5$, $M_2 = 63^{-1} \mod 8 = 7^{-1} \mod 8 = 7$ and $M_3 = 72^{-1} \mod 7 = 2^{-1} \mod 7 = 4$. One solution is then given by

$$x = (1 \cdot 56 \cdot 5 + 2 \cdot 63 \cdot 7 + 3 \cdot 72 \cdot 4) \mod 504 = 2026 \mod 504 = 10$$

and the rest are $504k + 10$ for $k \in \mathbb{Z}$.

**31.5-3** Denote by $x = a^{-1} \mod n$ and $x_i = x \mod n_i$. Since $ax \mod n = 1$ that means $ax \mod n_i = 1$ for every $n_i$. But since $a = c_1 a_1 + \ldots + c_k a_k$ and $n_i \mid c_j$ for every $j \neq i$, it further implies that

$$1 = ax \mod n_i = (c_1 a_1 + \ldots + c_k a_k)x \mod n_i = c_i a_i x \mod n_i = a_i x \mod n_i$$

since $c_i \mod n_i = (m_i(m_i^{-1} \mod n_i)) \mod n_i = 1$. Now if $x_i = x \mod n_i$, previous equation implies $a_i x_i \mod n_i = 1$.

Otherwise, let $x$ be the number such that $x_i := x \mod n_i = a_i^{-1} \mod n_i$. Then $x = p_i n_i + x_i$, for some $p_i$ and

$$ax = \sum_{l=1}^{k} a_l c_l (p_l n_l + x_l) = \sum_{l=1}^{k} a_l m_l M_l (p_l n_l + x_l) \equiv_{n_i} a_i m_i M_i x_i = 1$$

where $M_i = m_i^{-1} \mod n_i$ and since $n_i \mid m_l$ for $i \neq l$. Then, $n_i \mid ax - 1$ and since $n_i$ are relative prime, it implies $n \mid ax - 1$ and $ax \mod n = 1$.

**31.6-1** Smallest primitive root is 2, since

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $i$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $2^i$ | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 |
| $2^i \mod 11$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |

and therefore

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 2 | 4 | 8 | 5 | 10 | 9 | 7 | 3 | 6 | 1 |
| $\mathrm{ind}_{11,2}(a)$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |

Now since $\mathrm{ord}_{11}(a) = 10/\gcd(\mathrm{ind}_{11,2}(a), 10)$ ($\phi(11) = 10$) we find:

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| $\mathrm{ord}_{11}(a)$ | 1 | 10 | 5 | 5 | 5 | 10 | 10 | 10 | 5 | 2 |

**31.6-2** Value of $p$ in $i$-th iteration is $a^{2^i}$.

**Algorithm 1** ModExp$(a, b, n)$

**Require:** $(b_k, b_{k-1}, \ldots, b_0)$, the binary representation of $b$.

$p := a$, $x := 1$
**for** $i = 0$ to $k$ **do**
  **if** $b_i = 1$ **then**
    $x := (p \cdot x) \mod n$
  **end if**
  $p := p^2 \mod n$
**end for**
**return** x

**31.6-3** Euler theorem implies $a^{\phi(n)} \equiv_n 1$. Denote $x = a^{\phi(n)-1}$. Then $ax \equiv_n 1$ implying $x = a^{\phi(n)-1} = a^{-1} \mod n$. Therefore, one can compute $a^{-1} :=$ MODULAR-EXPONENTIATION$(a, \phi(n)-1, n)$.

**31.7-3** By definition of $P_A(M) = M^e \mod n$, we have that

$$P_A(M_1)P_A(M_2) = M_1^e M_2^e \mod n = (M_1 M_2)^e \mod n = P_A(M_1 M_2)$$

Let $C$ be the ciphertext and $Dec$ is the set of ciphers, adversary can decrypt. He should follow the procedure:

(1) $i := 0$
(2) If $C \in Dec$, decrypt it. Let $M$ be message.
(3) Choose random $x_i$ and compute $C := C \cdot P_A(x_i)$
(4) $i := i + 1$ and go to step 1
(5) Return $M x_{i-1}^{-1} \cdots x_0^{-1} \mod n$

Inverses modulo $n$ can be obtained by Modular-Exponentiation, since $x^{-1} \mod n = x^{n-2} \mod n$. Since $Dec$ contains about 1/100-th part of all ciphers, it would need about 100 iterations of the previous algorithm to terminate. So adversary can do the last step in reasonable time.

**31.8-3** Let $p$ be arbitrary prime and $\alpha, m$ integers. Denote by $p^\alpha \parallel m$ if $p^\alpha \mid m$ but $p^{\alpha+1} \nmid m$. Since $x^2 \equiv_n 1$ then $n \mid x^2 - 1$ and $\gcd(x^2-1, n) = n$. On the other hand, $p^\alpha \parallel x - 1$, $p^\beta \parallel x + 1$ and $p^\gamma \parallel n$, then $p^{\min\{\alpha,\gamma\}} \parallel \gcd(x-1, n)$ and $p^{\min\{\beta,\gamma\}} \parallel \gcd(x+1, n)$. On the other hand, since $x^2 - 1 = (x-1)(x+1)$, we have $p^{\alpha+\beta} \parallel x^2 - 1$ and hence $p^{\min\{\alpha+\beta,\gamma\}} \parallel \gcd(x^2-1, n)$. Since $\min\{\alpha,\gamma\} + \min\{\beta,\gamma\} \geq \min\{\alpha+\beta,\gamma\}$, and previous equations holds for arbitrary prime $p$, we conclude that

$$n = \gcd(x^2-1, n) \mid \gcd(x-1, n)\gcd(x+1, n)$$

Now since $1 < x < n - 1$, neither $\gcd(x-1, n)$ nor $\gcd(x+1, n)$ cannot be $n$. Therefore, if either of these factors is 1, previous equation implies that the other is $n$, which is contradiction. Hence, they are both in $(1, n)$ and hence non-trivial.