Solution of Problem 1

Let $a$ be a primitive element modulo $n$, i.e., $\mathbb{Z}_n^* = \{a^1, a^2, \ldots, a^{\varphi(n)} \equiv 1 \equiv a^0\}$.

Let $j \in \{1, \ldots, \varphi(n) - 1\}$ and $b = a^j \pmod{n}$. Then,

$$b$$ is a primitive element modulo $n$$\iff b^k \not\equiv 1 \pmod{n}, \forall k = 1, \ldots, \varphi(n) - 1 \land b^{\varphi(n)} \equiv 1 \pmod{n}$$

$$\iff a^{jk} \not\equiv 1 \pmod{n}, \forall k = 1, \ldots, \varphi(n) - 1 \land a^{j\varphi(n)} \equiv 1 \pmod{n}$$

$$\Rightarrow a^{jk} \not\equiv a^0 \pmod{n}$$

Therefore, $jk \not\equiv 0 \pmod{\varphi(n)}$ is necessary.

Proof of (2):

"⇒" Assume $\gcd(j, \varphi(n)) = c > 1$:

$$\left\lfloor \frac{\varphi(n)}{c} \right\rfloor \cdot j \equiv \varphi(n) \cdot \frac{j}{c} \equiv 0 \pmod{\varphi(n)},$$

but $jk \not\equiv 0 \pmod{\varphi(n)}, \forall k \in \{1, \ldots, \varphi(n) - 1\}$ is a contradiction. ¥

"⇐" Assume $\gcd(j, \varphi(n)) = 1$:

⇒ $j$ is invertible modulo $\varphi(n)$

⇒ $\exists l \in \mathbb{Z} : jl \equiv 1 \pmod{\varphi(n)}$.

Assume: $jk \equiv 0 \pmod{\varphi(n)}$ for some $k \in \{1, \ldots, \varphi(n) - 1\}$:

⇒ $l \cdot 0 = l \cdot j \cdot k \pmod{\varphi(n)}$

⇒ $0 \equiv k \pmod{\varphi(n)}$,

But $0 \not\in \{1, \ldots, \varphi(n) - 1\}$ is a contradiction. ¥

Thus, $jk \not\equiv 0 \pmod{\varphi(n)}$ is necessary.

• Altogether, $a^j$ is a primitive element modulo $n \iff \gcd(j, \varphi(n)) = 1$.

• The number of primitive elements modulo $n$ is equal to:

$$|\{j \in \{1, \ldots, \varphi(n) - 1\} | \gcd(j, \varphi(n)) = 1\}| = \varphi(\varphi(n)).$$
Solution of Problem 2
Shamir’s no-key protocol with the parameters: $p = 31337, a = 9999, b = 1011, m = 3567.$

a)

\[ c_1 = m^a \mod p = 3567^{9999} \mod 31337 \equiv 6399 \]  
\[ c_2 = c_1^b \mod p = 6399^{1011} \mod 31337 \equiv 29872 \ \text{(given by hint)} \]  
\[ c_3 = c_2^{a-1} \mod p = 29872^{14767} \mod 31337 \equiv 24982 \]  

To compute $c_1$ we use the square-and-multiply algorithm (SAM) (in chart):
The binary representation of $a = 9999$ is $10011100001111_2$.

**Hint:** If your calculator can not convert a large number $\Rightarrow$ convert it by hand.

For illustration, we can represent the exponentiation in terms of squareings by:

\[ m^a \equiv (\ldots (m^1)^2 m^0)^2 m^1)^2 m^1 \mod p \]

<table>
<thead>
<tr>
<th>op</th>
<th>exp</th>
<th>modulo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>3567</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>667</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>6171</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>13498</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>23177</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>3298</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>2865</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>29268</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>18929</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>31120</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>143</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>20384</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>30182</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>6399</td>
</tr>
</tbody>
</table>

**Hint:** Feel free to implement the SAM in order to check your results.

To compute $a^{-1}$ modulo $p - 1$, we use the EEA:

\[ 31336 = 3 \cdot 9999 + 1339 \]
\[ 9999 = 7 \cdot 1339 + 626 \]
\[ 1339 = 2 \cdot 626 + 87 \]
\[ 626 = 7 \cdot 87 + 17 \]
\[ 87 = 5 \cdot 17 + 2 \]
\[ 17 = 8 \cdot 2 + 1 \Rightarrow \gcd(31336, 9999) = 1 \]

To compute the inverse of $a$, we reorganize the last equation w.r.t. the remainder one
and substitute the factors backwards:

\[ 1 = 17 - 8 \cdot 2 \]
\[ = 17 - 8 \cdot (87 - 5 \cdot 17) = 41 \cdot 17 - 8 \cdot 87 \]
\[ = 41 \cdot 626 - 295 \cdot 87 \]
\[ = 631 \cdot 626 - 295 \cdot 1339 \]
\[ = 631 \cdot 9999 - 4712 \cdot 1339 \]
\[ = \left( \frac{14767 \cdot 9999 - 4712 \cdot 31336}{a^{-1}} \right) \cdot \frac{a}{a} \]

**Hint:** Check if result is equal to one in each step!

The computation of \( c_a^{-1} \mod p = 29872^{14767} \mod 31337 \) with SAM provides:

<table>
<thead>
<tr>
<th>op</th>
<th>exp</th>
<th>modulo</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>29872</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>9607</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>15639</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>24373</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>18957</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>16656</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>26421</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>6229</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>8290</td>
</tr>
<tr>
<td>S</td>
<td>0</td>
<td>2059</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>28387</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>13917</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>9317</td>
</tr>
<tr>
<td>SM</td>
<td>1</td>
<td>24982</td>
</tr>
</tbody>
</table>
Solution of Problem 3

a) The public parameters and the received ciphertext are:

- $e = d^{-1} \mod \varphi(n)$,
- $n = pq$,
- $c = m^e \mod n$.

The plaintext $m$ is not relatively prime to $n$, i.e., $p \mid m$ or $q \mid m$ and $p \neq q$.

Hence, gcd$(m, n) \in \{p, q\}$ holds. The gcd$(m, n)$ can be easily computed such that both primes can be calculated by either $q = \frac{n}{p}$ or $p = \frac{n}{q}$.

The private key $d$ can be computed since the factorization of $n = pq$ is known.

$$d = e^{-1} \mod \varphi(pq) = e^{-1} \mod (p - 1)(q - 1).$$

This inverse is computed using the extended Euclidean algorithm.

b) $m, n$ have common divisors.

The number of relatively prime numbers to $n$ are \(\varphi(n) = (p - 1)(q - 1) = pq - (p + q) + 1\).

$$P(\text{gcd}(m, n) = 1) = \frac{\varphi(n)}{n - 1}.$$ 

The complementary probability is computed by:

$$P = P(\text{gcd}(m, n) \neq 1) = 1 - \frac{\varphi(n)}{n - 1} = \frac{n - 1 - \varphi(n)}{n - 1} = \frac{pq - p q + p + q - 2}{p q - 1} = \frac{p + q - 2}{p q - 1}.$$ 

$c)$ $n : 1024$ Bits $\Rightarrow p \approx \sqrt{n} = 2^{512}, q \approx \sqrt{n} = 2^{512}$. From (b) we compute:

$$P = \frac{2^{512} + 2^{512} - 2}{2^{1024} - 1} = \frac{2^{513} - 2}{2^{1024} - 1} \approx 2^{-511} = (2^{-10})^{51} 2^{-1} \approx (10^{-3})^{51} \frac{5}{10} = 5 \cdot 10^{-154}$$

In general: $n = 2^k, p, q \approx 2^k$ for $k$ Bits.

$$P = \frac{2^k + 2^k - 2}{2^k - 1} = \frac{2^{k+1} - 2}{2^k - 1} \approx 2^{k+1}2^{-k} = 2^{-k+1}.$$ 

Thus, the probability that $m$ and $n$ are coprime is marginal, if $n$ has sufficiently many bits.
Solution of Problem 4

a) \( \varphi(n) = (u - 1)(v - 1) \), since \( u \) and \( v \) are distinct and prime.
\[
x^{\varphi(n)/2} \equiv x^{(u-1)(v-1)/2} \equiv (x^{u-1})(v-1)/2 \equiv 1^{(v-1)/2} \equiv 1 \pmod{u}
\]

Since \( v \) is an odd prime, it holds \( 2|(v-1) \) so that \( (v-1)/2 \) is an integer.

(Remark: Note that \( (x^{1/2})^{\varphi(n)} \pmod{n} \) is not defined!)

With analogous arguments, \( x^{\varphi(n)/2} \equiv 1 \pmod{v} \) is computed.

b) Since, \( u \) and \( v \) are coprime, we may apply the Chinese Remainder Theorem (solution is \( r \equiv x^{\varphi(n)/2} \pmod{n} \):
\[
x^{\varphi(n)/2} \equiv 1 \pmod{u},
x^{\varphi(n)/2} \equiv 1 \pmod{v},
\]
\[
M = pq,
M_1 = v, y_1 = v^{-1} \pmod{u},
M_2 = u, y_1 = u^{-1} \pmod{v}
\]
\[
r = (1 \cdot v \cdot (v^{-1} \pmod{u}) + 1 \cdot u \cdot (u^{-1} \pmod{v})) \pmod{u \cdot v}
= (v(v^{-1} \pmod{u}) + u(u^{-1} \pmod{v})) \pmod{u \cdot v}
= 1 , \text{ from definition of gcd}(u, v) = 1
\]

Note that since gcd\((u, v) = 1\) holds, it follows from the Extended Euclidean Algorithm, that \( ux + vy = \gcd(u, v) = 1 \). The unique solutions for \( x \) and \( y \) are \( x \equiv u^{-1} \pmod{v} \) and \( y \equiv v^{-1} \pmod{u} \). (cf. lecture section 'The Extended Euclidean Algorithm')

c) If \( ed \equiv 1 \pmod{\frac{1}{2}\varphi(n)} \) it follows that:
\[
ed = 1 + \frac{1}{2}\varphi(n)k, \ k \in \mathbb{Z},
\]
\[
\Leftrightarrow x^{ed} \equiv x^{1+\frac{1}{2}\varphi(n)k}
\]
\[
\equiv x(x^{\frac{1}{2}\varphi(n)})^k
\]
\[
\equiv x \cdot 1^k \equiv x \pmod{n}
\]