CS250: Discrete Math for Computer Science

L27: Cryptography and RSA
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:** $f_a : \mathbb{Z}_p^* \overset{1:1}{\longrightarrow} \mathbb{Z}_p^*$
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:**

$f_a : \mathbb{Z}_p^* \xrightarrow{1:1} \mathbb{Z}_p^*$

$f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x)$
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:**

$f_a : \mathbb{Z}_p^* \xrightarrow{1:1 \text{ onto}} \mathbb{Z}_p^*$

$f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x)$

$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$
Recall: Fermat’s Little Theorem

**Thm:** For \( p \) prime, \( a \in \mathbb{Z}_p^* \), \( a^{p-1} \equiv 1 \pmod{p} \)

**Proof:**

\[ f_a : \mathbb{Z}_p^* \xrightarrow{1:1} \text{onto} \mathbb{Z}_p^* \]

\[ f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x) \]

\[ \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\} \]

\[ \{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \]
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:**

$f_a : \mathbb{Z}_p^* \xrightarrow{1:1} \text{onto} \mathbb{Z}_p^*$

$f_a(x) = (a \cdot x)$  
$f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x)$

$\mathbb{Z}_p^* = \{1, 2, \ldots, p - 1\} = \{f_a(1), f_a(2), \ldots, f_a(p - 1)\}$

$\{1, 2, \ldots, p - 1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p - 1)\}$

$$\prod_{i \in \mathbb{Z}_p^*} i \equiv \prod_{i \in \mathbb{Z}_p^*} a \cdot i \pmod{p}$$
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:**
\[ f_a : \mathbb{Z}_p^* \xrightarrow{1:1} \text{onto} \mathbb{Z}_p^* \]
\[ f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x) \]
\[ \mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\} \]
\[ \{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\} \]
\[ \prod_{i \in \mathbb{Z}_p^*} i \equiv \prod_{i \in \mathbb{Z}_p^*} a \cdot i \pmod{p} \]
\[ \prod_{i \in \mathbb{Z}_p^*} i \equiv a^{p-1} \prod_{i \in \mathbb{Z}_p^*} i \pmod{p} \]
Recall: Fermat’s Little Theorem

**Thm:** For $p$ prime, $a \in \mathbb{Z}_p^*$, $a^{p-1} \equiv 1 \pmod{p}$

**Proof:**

$$f_a : \mathbb{Z}_p^* \xrightarrow{1:1} \mathbb{Z}_p^*$$

$$f_a(x) = (a \cdot x) \quad f_a^{-1}(x) = ((a^{-1} \pmod{p}) \cdot x)$$

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} = \{f_a(1), f_a(2), \ldots, f_a(p-1)\}$$

$$\{1, 2, \ldots, p-1\} = \{a \cdot 1, a \cdot 2, \ldots, a \cdot (p-1)\}$$

$$\prod_{i \in \mathbb{Z}_p^*} i \equiv \prod_{i \in \mathbb{Z}_p^*} a \cdot i \pmod{p}$$

$$\prod_{i \in \mathbb{Z}_p^*} i \equiv a^{p-1} \prod_{i \in \mathbb{Z}_p^*} i \pmod{p}$$

$$1 \equiv a^{p-1} \pmod{p} \quad \square$$
Euler’s phi function, $\varphi(n) = |\mathbb{Z}_n^*|$
Euler’s phi function, $\varphi(n) = |\mathbb{Z}_n^*|$

<table>
<thead>
<tr>
<th>$n$</th>
<th>$\varphi(n)$</th>
<th>$n$</th>
<th>$\varphi(n)$</th>
<th>$n$</th>
<th>$\varphi(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,

\[ \varphi(p) = p - 1 \]
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,

\[
\varphi(p) = p - 1
\]

\[
\varphi(p^{k+1}) = (p - 1)p^k
\]
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

**What’s the pattern?**

For \( p \) prime,

\[
\varphi(p) = p - 1
\]

\[
\varphi(p^{k+1}) = (p - 1)p^k
\]

If \( \gcd(a, b) = 1 \),

\[
\varphi(ab) = \varphi(a)\varphi(b)
\]
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,
\[
\varphi(p) = p - 1
\]
\[
\varphi(p^{k+1}) = (p - 1)p^k
\]

If \( \gcd(a, b) = 1 \),
\[
\varphi(ab) = \varphi(a)\varphi(b)
\]

Why?
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,

\[
\varphi(p) = p - 1
\]

\[
\varphi(p^{k+1}) = (p - 1)p^k
\]

If \( \gcd(a, b) = 1 \),

\[
\varphi(ab) = \varphi(a)\varphi(b)
\]

Why?
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,

\[
\varphi(p) = p - 1 \\
\varphi(p^{k+1}) = (p - 1)p^k
\]

If \( \gcd(a, b) = 1 \),

\[
\varphi(ab) = \varphi(a)\varphi(b)
\]

Why? CRT, hw5
Euler’s phi function, \( \varphi(n) = |\mathbb{Z}_n^*| \)

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
<th>( n )</th>
<th>( \varphi(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>1</td>
<td>11</td>
<td>10</td>
<td>20</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>12</td>
<td>4</td>
<td>21</td>
<td>12</td>
</tr>
<tr>
<td>4</td>
<td>2</td>
<td>13</td>
<td>12</td>
<td>22</td>
<td>10</td>
</tr>
<tr>
<td>5</td>
<td>4</td>
<td>14</td>
<td>6</td>
<td>23</td>
<td>22</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>15</td>
<td>8</td>
<td>24</td>
<td>8</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>16</td>
<td>8</td>
<td>25</td>
<td>20</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
<td>17</td>
<td>16</td>
<td>26</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>6</td>
<td>18</td>
<td>6</td>
<td>27</td>
<td>18</td>
</tr>
<tr>
<td>10</td>
<td>4</td>
<td>19</td>
<td>18</td>
<td>28</td>
<td>12</td>
</tr>
</tbody>
</table>

What’s the pattern?

For \( p \) prime,
\[
\varphi(p) = p - 1
\]
\[
\varphi(p^{k+1}) = (p - 1)p^k
\]

If \( \gcd(a, b) = 1 \),
\[
\varphi(ab) = \varphi(a)\varphi(b)
\]

Why?
CRT, hw5

For primes, \( p \neq q \),
\[
\varphi(pq) = (p - 1)(q - 1)
\]
Euler’s Thm:

For $m > 1$, $a \in \mathbb{Z}_m^*$, $a^{\varphi(m)} \equiv 1 \pmod{m}$. 
Euler’s Thm:

For $m > 1$, $a \in \mathbb{Z}_m^*$, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

**proof:** For $a \in \mathbb{Z}_m^*$, $f_a : \mathbb{Z}_m^* \xrightarrow{1:1} \mathbb{Z}_m^*$, $f_a(x) = (a \cdot x) \% m$
Euler’s Thm:

For $m > 1$, \( a \in \mathbb{Z}_m^* \), \( a^{\varphi(m)} \equiv 1 \pmod{m} \).

**proof:** For \( a \in \mathbb{Z}_m^* \), \( f_a : \mathbb{Z}_m^* \xrightarrow{1:1 \text{ onto}} \mathbb{Z}_m^* \), \( f_a(x) = (a \cdot x) \% m \)

\[
\mathbb{Z}_m^* = \{ b_1, \ldots, b_{\varphi(m)} \} = \{ f_a(b_1), \ldots, f_a(b_{\varphi(m)}) \}
\]
Euler’s Thm:

For \( m > 1, \ a \in \mathbb{Z}_m^*, \ a^{\varphi(m)} \equiv 1 \pmod{m} \).

**proof:** For \( a \in \mathbb{Z}_m^* \), \( f_a : \mathbb{Z}_m^* \xrightarrow{1:1 \text{ onto}} \mathbb{Z}_m^*, \ f_a(x) = (a \cdot x) \% m \)

\[
\mathbb{Z}_m^* = \{ b_1, \ldots, b_{\varphi(m)} \} = \{ f_a(b_1), \ldots, f_a(b_{\varphi(m)}) \}
\]

\[
\{ b_1, \ldots, b_{\varphi(m)} \} = \{ a \cdot b_1, \ldots, a \cdot b_{\varphi(m)} \}
\]
Euler’s Thm:

For $m > 1$, $a \in \mathbb{Z}_m^*$, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

**proof:** For $a \in \mathbb{Z}_m^*$, $f_a : \mathbb{Z}_m^* \overset{1:1}{\onto} \mathbb{Z}_m^*$, $f_a(x) = (a \cdot x) \% m$

\[\mathbb{Z}_m^* = \{b_1, \ldots, b_{\varphi(m)}\} = \{f_a(b_1), \ldots, f_a(b_{\varphi(m)})\}\]

\[\{b_1 \ldots, b_{\varphi(m)}\} = \{a \cdot b_1, \ldots, a \cdot b_{\varphi(m)}\}\]

\[\prod_{b \in \mathbb{Z}_m^*} b \equiv \prod_{b \in \mathbb{Z}_m^*} a \cdot b \pmod{m}\]
Euler’s Thm:

For \( m > 1 \), \( a \in \mathbb{Z}_m^* \), \( a^{\varphi(m)} \equiv 1 \pmod{m} \).

**proof:** For \( a \in \mathbb{Z}_m^* \), \( f_a : \mathbb{Z}_m^* \xrightarrow{\text{1:1 onto}} \mathbb{Z}_m^* \), \( f_a(x) = (a \cdot x) \% m \)

\[
\mathbb{Z}_m^* = \{ b_1, \ldots, b_{\varphi(m)} \} = \{ f_a(b_1), \ldots, f_a(b_{\varphi(m)}) \}
\]

\[
\{ b_1, \ldots, b_{\varphi(m)} \} = \{ a \cdot b_1, \ldots, a \cdot b_{\varphi(m)} \}
\]

\[
\prod_{b \in \mathbb{Z}_m^*} b \equiv \prod_{b \in \mathbb{Z}_m^*} a \cdot b \pmod{m}
\]

\[
\prod_{b \in \mathbb{Z}_m^*} b \equiv a^{\varphi(m)} \prod_{b \in \mathbb{Z}_p^*} b \pmod{m}
\]
Euler’s Thm:

For $m > 1$, $a \in \mathbb{Z}_m^*$, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

**proof:** For $a \in \mathbb{Z}_m^*$, $f_a : \mathbb{Z}_m^* \overset{1:1}{\rightarrow} \mathbb{Z}_m^*$, $f_a(x) = (a \cdot x) \% m$

$\mathbb{Z}_m^* = \{b_1, \ldots, b_{\varphi(m)}\} = \{f_a(b_1), \ldots, f_a(b_{\varphi(m)})\}$

$\{b_1 \ldots, b_{\varphi(m)}\} = \{a \cdot b_1, \ldots, a \cdot b_{\varphi(m)}\}$

$$\prod_{b \in \mathbb{Z}_m^*} b \equiv \prod_{b \in \mathbb{Z}_m^*} a \cdot b \pmod{m}$$

$$\prod_{b \in \mathbb{Z}_m^*} b \equiv a^{\varphi(m)} \prod_{b \in \mathbb{Z}_p^*} b \pmod{m}$$

$$1 \equiv a^{\varphi(m)} \pmod{m} \qed$$
One-Time Pad: a perfectly secure cryptosystem

\[ E(p, x) = p \oplus x \]

\[ D(p, x) = p \oplus x \oplus p = x = m \]

Encryption and decryption functions are the same: bitwise exclusive or with random, secret one-time pad, \( p \).
One-Time Pad: a perfectly secure cryptosystem
One-Time Pad: a perfectly secure cryptosystem

\[ p \in \{0, 1\}^n \quad m \in \{0, 1\}^n \quad = \quad \text{binary strings of length } n \]
One-Time Pad: a perfectly secure cryptosystem

\[ p \in \{0, 1\}^n \quad m \in \{0, 1\}^n = \text{binary strings of length } n \]

\[ E(p, x) = p \oplus x \]
One-Time Pad: a perfectly secure cryptosystem

\[ p \in \{0, 1\}^n \quad m \in \{0, 1\}^n = \text{binary strings of length } n \]

\[ E(p, x) = p \oplus x \]

\[ D(p, x) = p \oplus x \]
One-Time Pad: a perfectly secure cryptosystem

- $p \in \{0, 1\}^n$
- $m \in \{0, 1\}^n = \text{binary strings of length } n$
- $E(p, x) = p \oplus x$
- $D(p, x) = p \oplus x$
- $D(p, E(p, m)) = p \oplus (p \oplus m) = m$
One-Time Pad: a perfectly secure cryptosystem

\[ p \in \{0, 1\}^n \quad m \in \{0, 1\}^n = \text{binary strings of length } n \]

\[ E(p, x) = p \oplus x \]

\[ D(p, x) = p \oplus x \]

\[ D(p, E(p, m)) = p \oplus (p \oplus m) = m \]

Encryption and decryption functions are the same: bitwise **exclusive or** with random, **secret** one-time pad, \( p \).
One-Time Pad, Continued

| $p$ | 0 1 1 0 0 1 0 1 0 1 |

\[ E(p, m) = p \oplus m \quad D(p, s) = p \oplus s \]
One-Time Pad, Continued

<table>
<thead>
<tr>
<th>$p$</th>
<th>0 1 1 0 0 1 0 1 0 1 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>0 0 0 0 1 1 1 1 1 1 1 0 0</td>
</tr>
</tbody>
</table>

\[
E(p, m) = p \oplus m \quad D(p, s) = p \oplus s
\]
One-Time Pad, Continued

<table>
<thead>
<tr>
<th>$p$</th>
<th>0 1 1 0 0 1 0 1 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>0 0 0 0 1 1 1 1 1 0 0</td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0 1 1 0 1 0 1 0 0 1</td>
</tr>
</tbody>
</table>

\[
E(p, m) = p \oplus m \quad \quad D(p, s) = p \oplus s
\]
### One-Time Pad, Continued

<table>
<thead>
<tr>
<th>$p$</th>
<th>0 1 1 0 0 1 0 1 0 1 1 0</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>0 0 0 0 1 1 1 1 1 0 0 0</td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0 1 1 0 1 0 1 0 0 1 0 1</td>
</tr>
<tr>
<td>$D(p, E(p, m))$</td>
<td>0 0 0 0 1 1 1 1 1 0 0 0</td>
</tr>
</tbody>
</table>

\[
E(p, m) = p \oplus m \\
D(p, s) = p \oplus s
\]
One-Time Pad, Continued

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$m$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$D(p, E(p, m))$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

$E(p, m) = p \oplus m \\
D(p, s) = p \oplus s$

**Thm:** If $p$ is chosen at random and known only by $A$ and $B$,
One-Time Pad, Continued

<table>
<thead>
<tr>
<th>$p$</th>
<th>0 1 1 0 0 1 0 1 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>0 0 0 0 1 1 1 1 1 0 0</td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0 1 1 0 1 0 1 0 0 1</td>
</tr>
<tr>
<td>$D(p, E(p, m))$</td>
<td>0 0 0 0 1 1 1 1 1 0 0</td>
</tr>
</tbody>
</table>

\[
E(p, m) = p \oplus m \quad \quad D(p, s) = p \oplus s
\]

**Thm:** If $p$ is **chosen at random** and **known only** by $A$ and $B$,
Then $E(p, m)$ provides **no information** about $m$
### One-Time Pad, Continued

<table>
<thead>
<tr>
<th></th>
<th>0</th>
<th>1</th>
<th>1</th>
<th>0</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
<th>0</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$m$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$D(p, E(p, m))$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

\[
E(p, m) = p \oplus m \quad \quad \quad D(p, s) = p \oplus s
\]

**Thm:** If $p$ is chosen at random and known only by $A$ and $B$, then $E(p, m)$ provides no information about $m$ except perhaps its length.
### One-Time Pad, Continued

<table>
<thead>
<tr>
<th>$p$</th>
<th>0 1 1 0 0 1 0 1 0 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$m$</td>
<td>0 0 0 0 1 1 1 1 1 0 0</td>
</tr>
<tr>
<td>$E(p, m)$</td>
<td>0 1 1 0 1 0 1 0 0 1</td>
</tr>
<tr>
<td>$D(p, E(p, m))$</td>
<td>0 0 0 0 1 1 1 1 1 0 0</td>
</tr>
</tbody>
</table>

$E(p, m) = p \oplus m \quad D(p, s) = p \oplus s$

**Thm:** If $p$ is **chosen at random** and **known only** by $A$ and $B$,

Then $E(p, m)$ provides **no information** about $m$ except perhaps its length.

**Do not use $p$ more than once!**
Public-Key Cryptography

[Diffie, Hellman, 1976] Using computational complexity,
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me,
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]

For slightly over 3 weeks, each day Rivest and Shamir came up with a new scheme to do public-key cryptography, . . . , and by the next morning Adleman had broken it.
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]

For slightly over 3 weeks, each day Rivest and Shamir came up with a new scheme to do public-key cryptography, . . . , and by the next morning Adleman had broken it. The 23rd scheme, Adleman couldn’t break.
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]

For slightly over 3 weeks, each day Rivest and Shamir came up with a new scheme to do public-key cryptography, . . . , and by the next morning Adleman had broken it. The 23rd scheme, Adleman couldn’t break.

This is the RSA Public-Key Algorithm that is used today in the SSL algorithm.
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]

For slightly over 3 weeks, each day Rivest and Shamir came up with a new scheme to do public-key cryptography, . . . , and by the next morning Adleman had broken it. The 23rd scheme, Adleman couldn’t break.

This is the RSA Public-Key Algorithm that is used today in the SSL algorithm

Lets your browser generate key to send order to Amazon
[Diffie, Hellman, 1976] Using computational complexity, publish key for sending secret messages to me, intractable for anyone but me to decode.

RSA [Rivest, Shamir, Adleman, 1976]

For slightly over 3 weeks, each day Rivest and Shamir came up with a new scheme to do public-key cryptography, . . . , and by the next morning Adleman had broken it. The 23rd scheme, Adleman couldn’t break.

This is the RSA Public-Key Algorithm that is used today in the SSL algorithm

Let’s your browser generate key to send order to Amazon without, we believe, divulging any useful information about your credit card number, or what you bought.
RSA

B chooses \( p, q \) \( n \)-bit primes, and \( e \), s.t. \( \gcd(e, \varphi(pq)) = 1 \)
B chooses \( p, q \) \( n \)-bit primes, and \( e \), s.t. \( \gcd(e, \varphi(pq)) = 1 \)

B publishes: \( pq, e \); keeps \( p, q \) secret.
RSA

$B$ chooses $p, q$ $n$-bit primes, and $e$, s.t. $\gcd(e, \varphi(pq)) = 1$

$B$ publishes: $pq, e$; keeps $p, q$ secret.

Using Euclid's algorithm, $B$ computes $d, k$, s.t.

$$ed + k\varphi(pq) = 1$$

[$\varphi(pq) = (p - 1)(q - 1)$].
RSA

B chooses \( p, q \) \( n \)-bit primes, and \( e \), s.t. \( \gcd(e, \varphi(pq)) = 1 \)

B publishes: \( pq, e \); keeps \( p, q \) secret.

Using Euclid’s algorithm, B computes \( d, k \), s.t.

\[
ed + k\varphi(pq) = 1
\]

\[
[\varphi(pq) = (p - 1)(q - 1)].
\]

[Break message into pieces shorter than \( 2n \) bits]
RSA

B chooses $p, q$ $n$-bit primes, and $e$, s.t. $\gcd(e, \varphi(pq)) = 1$

B publishes: $pq, e$; keeps $p, q$ secret.

Using Euclid’s algorithm, B computes $d, k$, s.t.

$$ed + k\varphi(pq) = 1 \quad [\varphi(pq) = (p - 1)(q - 1)].$$

[Break message into pieces shorter than $2n$ bits]

$$E_B(x) \equiv x^e \pmod{pq}$$
B chooses \( p, q \) \( n \)-bit primes, and \( e \), s.t. \( \gcd(e, \varphi(pq)) = 1 \)

B publishes: \( pq, e \); keeps \( p, q \) secret.

Using Euclid’s algorithm, B computes \( d, k \), s.t.

\[
ed + k\varphi(pq) = 1 \quad \text{[} \varphi(pq) = (p - 1)(q - 1) \text{]}
\]

[Break message into pieces shorter than \( 2n \) bits]

\[
E_B(x) \equiv x^e \pmod{pq} \quad \text{and} \quad D_B(x) \equiv x^d \pmod{pq}
\]
B chooses $p, q$ $n$-bit primes, and $e$, s.t. $\gcd(e, \varphi(pq)) = 1$

B publishes: $pq, e$; keeps $p, q$ secret.

Using Euclid’s algorithm, $B$ computes $d, k$, s.t.
\[ ed + k\varphi(pq) = 1 \]

[Break message into pieces shorter than $2n$ bits]

\[
\begin{align*}
E_B(x) & \equiv x^e \pmod{pq} \\
D_B(x) & \equiv x^d \pmod{pq} \\
D_B(E_B(m)) & \equiv (m^e)^d \pmod{pq}
\end{align*}
\]
B chooses $p, q$ $n$-bit primes, and $e$, s.t. $\gcd(e, \varphi(pq)) = 1$

B publishes: $pq, e$; keeps $p, q$ secret.

Using Euclid’s algorithm, $B$ computes $d, k$, s.t.

$$ed + k\varphi(pq) = 1$$

$$[\varphi(pq) = (p - 1)(q - 1)].$$

[Break message into pieces shorter than $2n$ bits]

$$E_B(x) \equiv x^e \pmod{pq}$$

$$D_B(x) \equiv x^d \pmod{pq}$$

$$D_B(E_B(m)) \equiv (m^e)^d \pmod{pq}$$

$$\equiv m^{1-k\varphi(pq)} \pmod{pq}$$
RSA

\textbf{B chooses} \( p, q \) \( n \)-bit primes, and \( e \), \ s.t. \( \gcd(e, \varphi(pq)) = 1 \)

\textbf{B publishes:} \( pq, e \); \ keeps \( p, q \) secret.

Using Euclid’s algorithm, \textbf{B computes} \( d, k \), \ s.t.

\[
\begin{align*}
ed + k\varphi(pq) &= 1 \\
[\varphi(pq) &= (p - 1)(q - 1)].
\end{align*}
\]

[Break message into pieces shorter than \( 2n \) bits]

\[
\begin{align*}
E_B(x) &\equiv x^e \pmod{pq} \\
D_B(x) &\equiv x^d \pmod{pq} \\
D_B(E_B(m)) &\equiv (m^e)^d \pmod{pq} \\
&\equiv m^{1-k\varphi(pq)} \pmod{pq} \\
&\equiv m \cdot (m^{\varphi(pq)})^{-k} \pmod{pq}
\end{align*}
\]
RSA

\textbf{B chooses} \( p, q \) \( n \)-bit primes, and \( e \), s.t. \( \gcd(e, \varphi(pq)) = 1 \)

\textbf{B publishes:} \( pq, e \); keeps \( p, q \) secret.

Using Euclid's algorithm, \( B \) \textbf{computes} \( d, k \), s.t.

\[ ed + k\varphi(pq) = 1 \quad \text{[\( \varphi(pq) = (p - 1)(q - 1) \).]}

[Break message into pieces shorter than \( 2n \) bits]

\[
E_B(x) \equiv x^e \pmod{pq} \\
D_B(x) \equiv x^d \pmod{pq} \\
D_B(E_B(m)) \equiv (m^e)^d \pmod{pq} \\
\equiv m^{1-k\varphi(pq)} \pmod{pq} \\
\equiv m \cdot (m^{\varphi(pq)})^{-k} \pmod{pq} \\
\equiv m \pmod{pq} \quad \text{by Euler's Thm}
\]
B chooses $p$, $q$ $n$-bit primes, and $e$, s.t. $\gcd(e, \varphi(pq)) = 1$

B publishes: $pq$, $e$; keeps $p$, $q$ secret.

Using Euclid’s algorithm, B computes $d$, $k$, s.t.

$$ed + k\varphi(pq) = 1 \quad \text{[\varphi(pq) = (p - 1)(q - 1)].}$$

[Break message into pieces shorter than $2n$ bits]

$$E_B(x) \equiv x^e \pmod{pq}$$

$$D_B(x) \equiv x^d \pmod{pq}$$

$$D_B(E_B(m)) \equiv (m^e)^d \pmod{pq}$$

$$\quad \equiv m^{1 - k\varphi(pq)} \pmod{pq}$$

$$\quad \equiv m \cdot (m^{\varphi(pq)})^{-k} \pmod{pq}$$

$$\quad \equiv m \pmod{pq} \quad \text{by Euler’s Thm}$$

$$\quad \equiv E_B(D_B(m)) \pmod{pq}$$
For sufficiently large $n$, $[n \geq 1000 \text{ bits is currently fine}]$, ...
For **sufficiently large** $n$, 

$[n \geq 1000 \text{ bits is currently fine}]$,

It is **widely believed**: $E_B(m)$ **divulges no useful information** about $m$ to anyone not knowing $p$, $q$, or $d$. 

---

**Message signing:**

Let $m = "B promises to give $A$ $10, valid until 12/17/16."$

Let $m' = m, r$, where $r$ is nonce or current date and time.

It is **widely believed** $D_B(m')$ could be produced only by $B$. Thus it can be used as a **contract signed by $B$**. Useful for proving **authenticity**.

**Public Key Cryptography** is a **theoretical underpinning** for possible computer security even over the web.
For **sufficiently large** \( n \), \([n \geq 1000 \text{ bits is currently fine}]\),
It is **widely believed**: \( E_B(m) \) divulges **no useful information**
about \( m \) to anyone not knowing \( p, q, \) or \( d \).

**Message signing:**
Let \( m = \text{“}B \text{ promises to give } A \text{ $10, valid until 12/17/16.”} \)
Let \( m' = m, r \) where \( r \) is nonce or current date and time.
For **sufficiently large** \( n \), \( n \geq 1000 \) bits is currently fine.

It is **widely believed**: \( E_B(m) \) divulges **no useful information** about \( m \) to anyone not knowing \( p \), \( q \), or \( d \).

**Message signing:**

Let \( m = \) “\( B \) promises to give \( A \) $10, valid until 12/17/16.”

Let \( m' = m, r \) where \( r \) is nonce or current date and time.

It is **widely believed** \( D_B(m') \) could be produced only by \( B \).
For sufficiently large $n$, \([n \geq 1000 \text{ bits is currently fine}]\),
It is widely believed: \(E_B(m)\) divulges no useful information
about \(m\) to anyone not knowing \(p, q,\) or \(d\).

**Message signing:**
Let \(m = \text{“B promises to give A $10, valid until 12/17/16.”}\)
Let \(m' = m, r\) where \(r\) is nonce or current date and time.
It is widely believed \(D_B(m')\) could be produced only by \(B\).
Thus it can be used as a **contract** signed by \(B\).
For sufficiently large $n$, $n \geq 1000$ bits is currently fine],
It is widely believed: $E_B(m)$ divulges no useful information
about $m$ to anyone not knowing $p$, $q$, or $d$.

**Message signing:**
Let $m = “B promises to give A $10, valid until 12/17/16.”$
Let $m' = m, r$ where $r$ is nonce or current date and time.

It is widely believed $D_B(m')$ could be produced only by $B$.
Thus it can be used as a **contract** signed by $B$.
Useful for proving **authenticity**.
For sufficiently large $n$, \[ n \geq 1000 \text{ bits is currently fine}, \]
It is widely believed: $E_B(m)$ divulges no useful information about $m$ to anyone not knowing $p$, $q$, or $d$.

**Message signing:**
Let $m = \text{“}B\text{ promises to give }A\text{ $10, valid until 12/17/16.\text{”}.$}
Let $m' = m, r$ where $r$ is nonce or current date and time.
It is widely believed $D_B(m')$ could be produced only by $B$.
Thus it can be used as a **contract** signed by $B$.
Useful for proving **authenticity**.

**Public Key Cryptography** is a theoretical underpinning for possible computer security even over the web.