CS456/556/MA456 Cryptography. Quiz 0 (take-home). Open book (no Turing machines)

Bob is using RSA public-key cryptography with modulus $n = 989$ and a one-bit salting (where the message is padded with a random low-order bit). He chooses the smallest valid odd integer for the public exponent e. One fine day, an encrypted salted message from Alice arrived: it was 983 (mod 989). *Circle the ASCII character that is Alice's actual message sent to Bob.*

<table>
<tr><td>0 NUL</td><td>1 SOH</td><td>2 STX</td><td>3 ETX</td><td>4 EOT</td><td>5 ENQ</td><td>6 ACK</td><td>7 BEL</td></tr>
<tr><td>8 BS</td><td>9 HT</td><td>10 NL</td><td>11 VT</td><td>12 NP</td><td>13 CR</td><td>14 SO</td><td>15 SI</td></tr>
<tr><td>16 DLE</td><td>17 DC1</td><td>18 DC2</td><td>19 DC3</td><td>20 DC4</td><td>21 NAK</td><td>22 SYN</td><td>23 ETB</td></tr>
<tr><td>24 CAN</td><td>25 EM</td><td>26 SUB</td><td>27 ESC</td><td>28 FS</td><td>29 GS</td><td>30 RS</td><td>31 US</td></tr>
<tr><td>32 SP</td><td>33 !</td><td>34 "</td><td>35 #</td><td>36 $</td><td>37 %</td><td>38 &</td><td>39 ’</td></tr>
<tr><td>40 (</td><td>41)</td><td>42 *</td><td>43 +</td><td>44 ,</td><td>45 -</td><td>46 .</td><td>47 /</td></tr>
<tr><td>48 0</td><td>49 1</td><td>50 2</td><td>51 3</td><td>52 4</td><td>53 5</td><td>54 6</td><td>55 7</td></tr>
<tr><td>56 8</td><td>57 9</td><td>58 :</td><td>59 ;</td><td>60 <</td><td>61 =</td><td>62 ></td><td>63 ?</td></tr>
<tr><td>64 @</td><td>65 A</td><td>66 B</td><td>67 C</td><td>68 D</td><td>69 E</td><td>70 F</td><td>71 G</td></tr>
<tr><td>72 H</td><td>73 I</td><td>74 J</td><td>75 K</td><td>76 L</td><td>77 M</td><td>78 N</td><td>79 O</td></tr>
<tr><td>80 P</td><td>81 Q</td><td>82 R</td><td>83 S</td><td>84 T</td><td>85 U</td><td>86 V</td><td>87 W</td></tr>
<tr><td>88 X</td><td>89 Y</td><td>90 Z</td><td>91 [</td><td>92 \</td><td>93]</td><td>94 ^</td><td>95 _</td></tr>
<tr><td>96 ‘</td><td>97 a</td><td>98 b</td><td>99 c</td><td>100 d</td><td>101 e</td><td>102 f</td><td>103 g</td></tr>
<tr><td>104 h</td><td>105 i</td><td>106 j</td><td>107 k</td><td>108 l</td><td>109 m</td><td>110 n</td><td>111 o</td></tr>
<tr><td>112 p</td><td>113 q</td><td>114 r</td><td>115 s</td><td>116 t</td><td>117 u</td><td>118 v</td><td>119 w</td></tr>
<tr><td>120 x</td><td>121 y</td><td>122 z</td><td>123 {</td><td>124 |</td><td>125 }</td><td>126 ~</td><td>127 DEL</td></tr>
</table>

- What are Bob's prime numbers $p < q$? What is his Euler constant $\phi(n)$?
- What are Bob's public and secret exponents e and d? Use the extended Euclidean algorithm.

$\phi(n) =$	$e =$	Q	R	x_1	y_1	x_2	y_2
				1	0	0	1

- (Decryption using Chinese Remainder Theorem) Alice's encrypted salted message is $M^e \equiv 983 \pmod{989}$. Compute $M \pmod{p}$ and $M \pmod{q}$ using Fermat's Little Theorem.

$$M \equiv \quad \ldots \quad \pmod{p}, \qquad M \equiv \quad \ldots \quad \pmod{q}$$

Use Chinese Remainder Theorem to recover $M \pmod{989}$ using the pulverizer.

$q =$	$p =$	Q	R	x_1	y_1	x_2	y_2
				1	0	0	1

Now, remove the low-order one-bit salt from M. Thus, Alice's actual ASCII message was $m \equiv \ldots \pmod{989}$.

- (CS556) Solve the following.
  1. Prove: If a prime p divides ab, for integers a and b, then p divides a or p divides b.
  2. Prove (Euler-Fermat): For every positive integer $n \geq 2$, if a satisfies $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Here, $\phi(n)$ denotes the number of integers between 1 and $n-1$ that are relatively prime to n.