<table>
<thead>
<tr>
<th>Lesson</th>
<th>Title</th>
<th>Primary Activities</th>
<th>Assessments</th>
</tr>
</thead>
</table>
| 1      | The Language of Cryptology & the Shift is On! | • Student as Agent-in-training  
• The importance of secrecy  
• Career opportunities  
• The terminology of codes  
• Deciphering a shift cipher  
• Introducing the cast of characters | • Survey of prior knowledge and opinions  
• Caesar shift enciphering/deciphering  
• Vocabulary check |
| 2      | Agent Training in Basic Arithmetic | • Multiplication algorithms/arrays  
• Distributive property  
• Division/remainders  
• Tests for divisibility  
• Parity and primeness | • Interpreting and making arrays  
• Vocabulary of multiplication and division  
• Solving for partial products and remainders  
• Recognizing factors  
• Recognizing parity and primeness |
| 3      | Codes That Use Keywords & Factoring | • De Vigenère ciphers  
• The method of public key  
• Squares and square roots  
• Trial division and spreadsheet  
• Prime factorization | • Keyword encoding and decoding  
• Factoring using trial division  
• Procedure writing |
| 4      | Cipher Formulas & Modular Arithmetic | • Atbash spreadsheet and formula  
• Clock arithmetic  
• Shift cipher formula  
• A need for modular arithmetic  
• Negative integers in mod 26 | • Writing modular notation  
• Caesar shift enciphering/deciphering using modulo 26  
• Solving time problems in mod 12  
• Performing arithmetic in other modular bases |
| 5 | Digital Roots & the Secret Digit Trick | - Learning and explaining a number trick  
- Problem constraints  
- Casting out nines (modulo 9 congruence)  
- Applying expanded notation and the distributive property  
- Error trapping/computer bugs | - Performing a subtraction trick  
- Explaining the trick using expanded form and distribution  
- Writing a script  
- Modeling constraints  
- Catching math errors |
| 6 | Affine Ciphers & Modular Inverses | - Affine enciphering  
- Mathematical limitations  
- Pigeonhole principle  
- Solving affine ciphers  
- Inverses in modular form  
- The inverse of composite operations | - Application of common factors and transforming the alphabet  
- Finding modular multiplicative inverses  
- Comparing multiplicative inverse forms  
- Enciphering and deciphering with affine formulas  
- Assessing affine weaknesses |
| 7 | Random Substitution & Cryptograms | - Permutations of the alphabet  
- Crypto-analysis using statistics; English language structures; frequency counts of letters; common words/phrases  
- A further weakness in shift ciphers | - Solving puzzles as an entry into cryptanalysis  
- Solving cryptograms and codeword puzzles  
- Making and analyzing frequency histograms  
- Using technology to aid in analysis  
- Comparing shift ciphers and the alphabet profile |
| 8 | Prime Secrets & Patterns Beware! | - Patterns in the square numbers  
- Counting prime frequencies  
- Investigating Euclid’s proof  
- The Multiplication Race  
- Fermat’s factoring method  
- Investigations into pattern breakers | - Pattern recognition and extension  
- Detecting pattern breaking  
- Paraphrasing Euclid’s proof  
- Mental calculation—sums and differences of squares  
- Variable representation of differences of squares  
- Performing and reporting investigations  
- Factoring and prime detecting |
<table>
<thead>
<tr>
<th></th>
<th>An Abundance of Factors or Not!</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Factor lists</td>
<td></td>
<td>Investigation into a perfect number pattern—report of findings</td>
</tr>
<tr>
<td></td>
<td>Prime factorization</td>
<td></td>
<td>Finding odd abundant numbers—report of findings</td>
</tr>
<tr>
<td></td>
<td>Factor counts by formula</td>
<td></td>
<td>Review of prime factorization</td>
</tr>
<tr>
<td></td>
<td>Factor sums</td>
<td></td>
<td>Unit Review, Part I – The Math</td>
</tr>
<tr>
<td></td>
<td>Factor abundance and deficiency</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Perfect numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Geometric dissections</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Odd abundant numbers</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A number trick with 1001</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Strengthening the Ciphers</td>
<td></td>
<td>Unit Review, Part II – The Codes</td>
</tr>
<tr>
<td></td>
<td>Summary and Reflections; Cryptarithms</td>
<td></td>
<td>Final skill and vocabulary check (Unit Test)</td>
</tr>
<tr>
<td></td>
<td>Cipher variations and security comparisons</td>
<td></td>
<td>Post survey of knowledge and opinions</td>
</tr>
<tr>
<td></td>
<td>Parting puzzles</td>
<td></td>
<td>Writing assignment—acceptable use policy for codes</td>
</tr>
<tr>
<td></td>
<td>Exit project—Ethics in cryptology</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>