Day 03 - Classical Cryptosystems (cont.)

Last time
- Generalize mono-alphabetic subs.
  
  (Caesar shift w/o keeping the ABC order)
  \[ |K| = 26! \]
- Vigenere cipher: need a keyword of length \( N \).
  Use multiple Caesar shifts.
  \[ \text{Keyword: YES} \]
  \[ \begin{align*}
  Y &= \text{shift of every 1st, 4th, 7th,... letters} \\
  E &= \text{shift of every 2nd, 5th, 8th,... letters} \\
  S &= \text{shift of every 3rd, 6th, 9th,... letters} 
  \end{align*} \]

- Rectangular Transposition:
  Put p/f into a rectangle & rearrange the columns.

\[
\begin{array}{c}
\text{Pla} \text{y} \text{f} \text{a} \text{i} \\
\text{r} \text{a} \\
\text{a} \text{i} \\
\text{r} \\
\text{a} \\
\text{i} \\
\text{a} \\
\text{r} \\
\text{i} \\
\text{a} \\
\text{r} \\
\text{i} \\
\text{a} \\
\text{r} \\
\text{i} \\
\text{a} \\
\text{r} \\
\end{array}
\]

\[
\begin{array}{c}
\text{N} \\
\text{O} \\
\text{W} \\
\text{A} \\
\text{Y} \\
\text{B} \\
\text{C} \\
\text{D} \\
\text{E} \\
\text{F} \\
\text{G} \\
\text{H} \\
\text{I} \\
\text{J} \\
\text{K} \\
\text{L} \\
\text{M} \\
\text{N} \\
\text{O} \\
\text{P} \\
\text{Q} \\
\text{R} \\
\text{T} \\
\text{U} \\
\text{V} \\
\text{X} \\
\text{Y} \\
\text{Z} \\
\end{array}
\]

- Encrypt: Same row: shift right \((GK \rightarrow HL, CF \rightarrow DB)\)
  - Same col: shift down \((PU \rightarrow UO, AR \rightarrow EX)\)
  - Corner: replace with the other corner \((PE: C \leftarrow E \rightarrow RC)\)

ADFGVX cipher
- The ADFGVX system was introduced by the German Colonel Fritz Nebel.
- It was broken by Georges Painvin in one of the all-time most remarkable feats of cryptanalysis.
- It was not until December 1932 that the feat of Painvin was made known.
- It permitted the French to block the last German offensive of 1918.
- ADFGVX can be seen as a combination between Playfair cipher and rectangular transposition.

Encryption process:
1. Construct a 6x6 ADFGVX matrix with entries taken from 26 alphabet letters and 10 number digits.
2. Convert each letter in the plaintext into its coordinates in the ADFGVX table. Coordinates are ordered as (row index, column index).
3. Rearrange the converted text (row-by-row from left to right) into a table with the columns and permute the columns using a chosen permutation of length 26.
4. Read the permuted table column by column from top to bottom to obtain the ciphertext.
4. Read the permuted table column by column from to bottom to obtain the ciphertext.
Decryption process:

1. Fill the letters of the cipher-text into a table of $n$ columns, where $n$ is the length of the permutation. We fill the entries column-by-column, top-to-bottom, and left-to-right.

2. Label each column from left to right with $1, 2, \ldots, n$. Then rearrange the column so that the given permutation appears.

3. Read the text from step 2 row-by-row, left-to-right, and top-to-bottom. Then break the resultant text into pairs.

4. Translate each pair into the plaintext using its coordinates in the AD-FGDX table. Coordinates are ordered as (row index, column index).
Vernam cipher

Theorem 1 (Quotient-Remainder Theorem). Given an integer \( A \) and a positive integer \( B \). Then there exist integers \( q \) and \( r \) (obtained through long division) such that
\[ A = qB + r, \quad 0 \leq r < B. \]

Here, \( q \) is quotient and \( r \) is remainder. We say \( A \equiv r \pmod B \).

Example.
\[
\begin{align*}
\quad \frac{521}{26} & = 20 \times 26 + 1 \\
\text{quotient} \quad \text{remainder} \\
-521 & = -26 \times 20 - 1 = 26 \times (-20) + (-1) \\
521 & \equiv 1 \pmod {26} \\
-521 & \equiv 25 \pmod {26}.
\end{align*}
\]

\[
\begin{align*}
521 + 264 & \equiv (\pmod {26}) \\
\downarrow \quad \downarrow \\
1 & \equiv 5 \pmod {26} \\
264 & \equiv 4 \pmod {26}
\end{align*}
\]

\[
\begin{align*}
139 \times 787 & \equiv (\pmod {26}) \\
\quad 9 \times 7 & \equiv 63 \quad (\pmod {26}) \\
787 & \equiv 11 \pmod {26}
\end{align*}
\]
Vernam cipher - Encryption process:

- Translate the given plaintext into numbers $A \rightarrow 0, B \rightarrow 1, \ldots, Z \rightarrow 25$.
- Randomize two short keys $U$ and $V$ and compute the long key $V'$ as follows:
  
  $$K(i) = U(i) + V(i) \mod 26$$

  for each $1 \leq i \leq n$ where $n$ is the length of the plaintext.
- Compute $C(i) = M(i) + K(i) \mod 26$ for each $i$, and we substitute each $M(i)$ by the corresponding letter in the alphabet.

**Example.** Encrypt the message NO MORE AMMO using the keys

\[ \{U, V\} = \{(3, 1, 2), (7, 7, 9, 5, 5, 9, 1)\} \]

Solution. The long key $K$ is

\[
\begin{array}{cccccccc}
U & 3 & 1 & 2 & 3 & 1 & 2 & 3 & 1 \\
V' & 7 & 3 & 8 & 4 & 5 & 7 & 3 & 8 & 4 & 5 \\
K & 10 & 4 & 10 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 12 & 14 \\
\end{array}
\]

\[
\begin{array}{cccccccc}
\text{Plaintext} & N & O & M & O & R & E & A & M & M & O \\
M & 13 & 14 & 12 & 14 & 17 & 4 & 0 & 12 & 12 & 14 \\
K & 10 & 4 & 10 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 6 & 9 & 12 & 14 \\
C & 23 & 18 & 22 & 21 & 23 \\
\text{Ciphertext} & X & S & W & V & X \\
\end{array}
\]
Definition 1 (Inverse in modular arithmetic). If $A \cdot C = 1 \pmod{B}$ then $C$ is the modular inverse of $A$ under $B$. Denote $C = A^{-1} \pmod{B}$.

Use the multiplication table to find the inverses under mod 26.

To find inverse of 5, look at row 5 and find a "1" entry in the table.

- If there's a "1" in the column number, then the inverse is the column number.
- If there's no "1" then the inverse D.N.E.