# CRYPTOGRAPHY HANDOUT 02

VIGENÈRE CIPHER

## 1. Number and Letter Correspondence (mod26)

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

## 2. Vigenère Table

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| S | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| T | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| Z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

https://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher

## 3. Frequencies of Letters in English

| a | b | c | d | e | f | g | h | i | j | k | l | m |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| .082 | .015 | .028 | .043 | .127 | .022 | .020 | .061 | .070 | .002 | .008 | .040 | .024 |
| n | o | p | q | r | s | t | u | v | w | x | y | z |
| .067 | .075 | .019 | .001 | .060 | .063 | .091 | .028 | .010 | .023 | .001 | .020 | .001 |

## 4. Vigenère Example

(From 2.3 in Trappe and Washington)

(V)VHQW(V)VRHM(U)SGJG(T)HKIH(T)SSEJ(C)HLSF(C)BGVW(C)RLRY(Q)TFSV(G)AHW
K(C)UHWA(U)GLQH(N)SLRL(J)SHBL(T)SPIS(P)RDXL(J)SVEE(G)HLQW(K)ASSK(U)WE
PW(Q)TWVS(P)GOEL(K)CQYF(N)SVWL(J)SNIQ(K)GNRG(Y)BWLW(G)OVIO(K)HKAZ(K)Q
KXZ(G)YHCE(C)MEIU(J)OQKW(F)WVEF(Q)HKIJ(R)CLRL(K)BIEN(Q)FRJL(J)SDHG(R)
HLSF(Q)TWLA(U)QRHW(D)MWLG(U)SGIK(K)FLRY(V)CWVS(P)GPML(K)ASSJ(V)OQXE
(G)GVEY(G)GZML(J)CXXL(J)SVPA(I)VWIK(V)RDRY(G)FRJL(J)SLVE(G)GVEY(G)GEI
A(P)UUIS(F)PBTG(N)WWMU(C)ZRVT(W)GLRW(U)GUMN(C)ZVIL(E)

See Frequency Analysis code.

### 4.1. **Key Length.**

1. Take the ciphertext and write it on two strips of paper.
2. Put one strip of paper above the other but displaced by a certain number of places.
3. Mark the number of times a letter and the one below it are the same.
4. Count the number of coincidences.

See last page for printout.

### 4.2. **Finding the Key: Method 2 (in text).** For $i = 1$ to $n$,

1. Compute frequencies of the letters in positions $i \bmod n$, and form the vector $\vec{W}$.
2. For $j = 1$ to 25, compute $\vec{W} \cdot \vec{A}_j$.
3. Let $k_i = j_0$ give the maximum value of $\vec{W} \cdot \vec{A}_j$.

The key is probably $\{k_1, k_2, k_3, \cdots, k_n\}$.

## 5. Vigenère Key Length Example

Print the following out, and cut into two strips. Then follow the instructions from Section 4.1.

VVHQWVVRHMUSGHGTHKIHT...

VVHQWVVRHMUSGHGTHKIHT...