The Vigenere Cipher: Blaise de Vigenere 16th Century (France)

Example: $K = \text{VECTOR} = (21,4,2,19,14,17)$

W	*E*	*W*	*I*	*L*	*L*	*M*	*E*	*E*	*T*	*A*	*T*	*M*	*I*	*D*	*N*	*I*	*G*	*H*	*T*
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19	14	17	21	4
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
17	8	24	1	25	2	7	8	6	12	14	10	7	12	5	6	22	23	2	23
R	*I*	*Y*	*B*	*Z*	*C*	*H*	*I*	*G*	*M*	*O*	*K*	*H*	*M*	*F*	*G*	*W*	*X*	*C*	*X*

Polyalphabetic vs Monoalphabetic Cipher

The Vigenere Cipher (1)

Cryptanalysis — Goal: Determine the keyword length *m*

The Kasiski test:

- search for pairs of identical segments of length at least three
- compute the distance between the starting positions of the two segments

$$m \quad \text{divides} \quad gcd(d_1, d_2, \ldots)$$

The Vigenere Cipher (2)

Cryptanalysis

The index of coincidence (Friedman):

$$\textit{Given } \boldsymbol{x}=x_1 x_2 \cdots x_n, \textit{ and } i, j \in_R \{1,2,\ldots n\},$$
$$\textit{then } I_c(\boldsymbol{x}) = P(x_i = x_j).$$

The Vigenere Cipher (3)

Cryptanalysis

$$A=0,\quad B=1,\quad C=2,\quad D=3,\quad \ldots\ldots,\quad Z=25$$
$$f_0,\qquad f_1,\qquad f_2,\qquad f_3,\qquad \ldots\ldots,\qquad f_{25}$$

$$\binom{n}{k}=\frac{n!}{k!(n-k)!};\qquad \binom{n}{2},\ \binom{f_i}{2}$$

The Vigenere Cipher (4)

Cryptanalysis

$$I_c(\boldsymbol{x}) = \frac{\binom{f_0}{2}+\cdots+\binom{f_{25}}{2}}{\binom{n}{2}} = \frac{\sum_{i=0}^{25} f_i(f_i-1)}{n(n-1)}$$

The Vigenere Cipher (5)

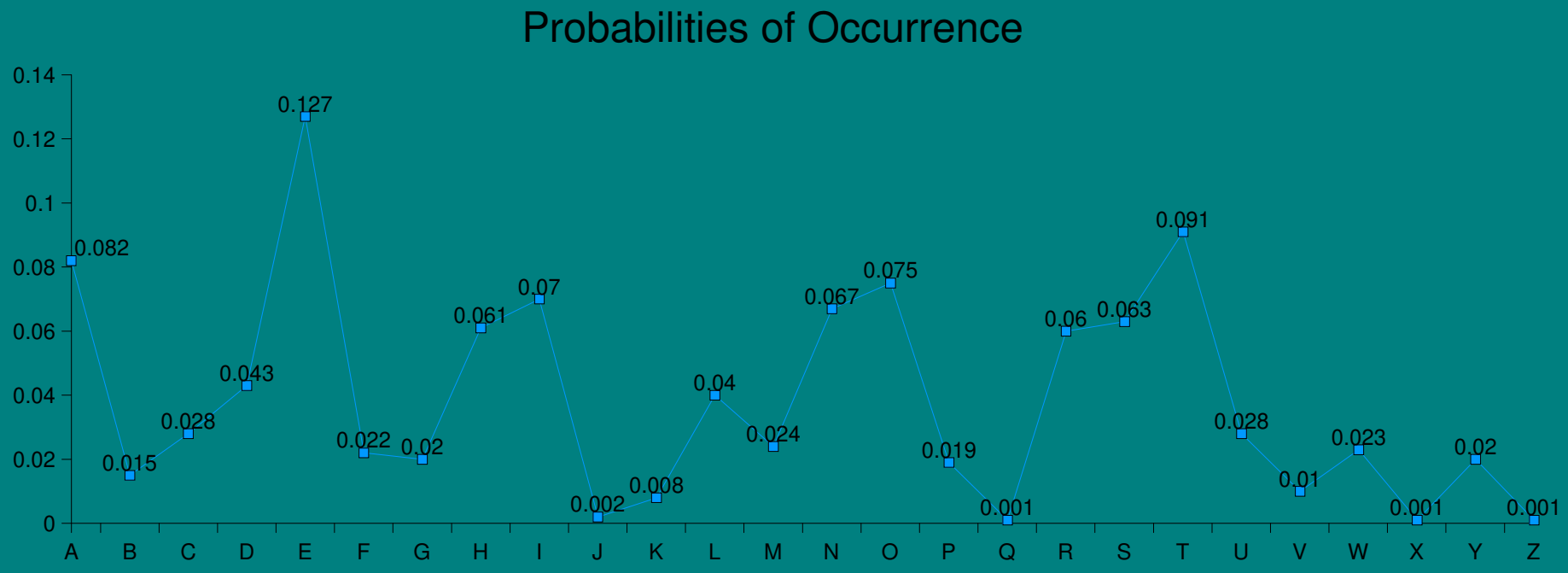
Cryptanalysis

$$I_c(\boldsymbol{x}) = \frac{\sum_{i=0}^{25} f_i(f_i - 1)}{n(n-1)} \approx \frac{\sum_{i=0}^{25} f_i(f_i)}{n(n)} =$$

$$= \sum_{i=0}^{25} \left(\frac{f_i}{n}\right)^2 = \sum_{i=0}^{25} p_i^2 = 0.065$$

The Vigenere Cipher (6)

Cryptanalysis



The Vigenere Cipher (7)

Cryptanalysis

$$\boldsymbol{y} = y_1 y_2 y_3 \cdots y_n$$

$$\begin{bmatrix} y_1 & y_{m+1} & y_{2m+1} & \cdots & y_{n-m+1} \\ y_2 & y_{m+2} & y_{2m+2} & \cdots & y_{n-m+2} \\ y_3 & y_{m+3} & y_{2m+3} & \cdots & y_{n-m+3} \\ \vdots & \vdots & \vdots & & \vdots \\ y_m & y_{2m} & y_{3m} & \cdots & y_n \end{bmatrix}$$

The Vigenere Cipher (8)

Cryptanalysis

$$
\begin{array}{lcccccc}
\boldsymbol{y_1} & = & y_1 & y_{m+1} & y_{2m+1} & \cdots & y_{n-m+1} \\
\boldsymbol{y_2} & = & y_2 & y_{m+2} & y_{2m+2} & \cdots & y_{n-m+2} \\
\boldsymbol{y_3} & = & y_3 & y_{m+3} & y_{2m+3} & \cdots & y_{n-m+3} \\
\vdots & & \vdots & \vdots & \vdots & & \vdots \\
\boldsymbol{y_m} & = & y_m & y_{2m} & y_{3m} & \cdots & y_n
\end{array}
$$

The Vigenere Cipher (9)

Cryptanalysis

$$I_c(\boldsymbol{x}) \approx \sum_{i=0}^{25} p_i^2 = 0.065$$

$$I_c(\boldsymbol{y_i}) \approx 0.065, \quad \forall\, 1 \leqslant i \leqslant m$$

$$I_c \approx \sum_{i=0}^{25} (1/26)^2 = 26(1/26)^2 = 0.038$$

The Vigenere Cipher (10)

Cryptanalysis $0.038 \Leftrightarrow 0.065$

$$[R\ I\ Y\ B\ Z\ C\ H\ I\ G\ M\ O\ K\ H\ M\ F\ G\ W\ X\ C\ X]$$

$$\begin{bmatrix} R & Y & Z & H & G & O & H & F & W & C \\ I & B & C & I & M & K & M & G & X & X \end{bmatrix}$$

$$\begin{bmatrix} R & B & H & M & H & G & C \\ I & Z & I & O & M & W & X \\ Y & C & G & K & F & X & \end{bmatrix}$$

$$\begin{bmatrix} R & Z & G & H & W \\ I & C & M & M & X \\ Y & H & O & F & C \\ B & I & K & G & X \end{bmatrix}$$

The Vigenere Cipher (11)

Cryptanalysis

Determine the keyword!

W	*E*	*W*	*I*	*L*	*L*	*M*	*E*	*E*	*T*	*A*	*T*	*M*	*I*	*D*	*N*	*I*	*G*	*H*	*T*
22	4	22	8	11	11	12	4	4	19	0	19	12	8	3	13	8	6	7	19
21	4	2	19	14	17	21	4	2	19	14	17	21	4	2	19	14	17	21	4
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
17	8	24	1	25	2	7	8	6	12	14	10	7	12	5	6	22	23	2	23
R	*I*	*Y*	*B*	*Z*	*C*	*H*	*I*	*G*	*M*	*O*	*K*	*H*	*M*	*F*	*G*	*W*	*X*	*C*	*X*

$$26^5 > 1.1 \times 10^7$$