CIFRARIO DI VIGENERE *prof.ssa Daniela Casale*

Il cifrario di **Vigenère** è un'estensione del cifrario di Leon Battista Alberti, che sappiamo nella seconda metà del 1400 aveva utilizzato due alfabeti per cifrare.

Vigenère decise invece di usarne 26, uno per ogni lettera dell'alfabeto. In questo modo ogni singola lettera della frase da cifrare viene crittata con un differente alfabeto, secondo una regola che viene decisa **dalla tavola di Vigenère e dalla parola chiave**. Anche in questo caso la chiave da utilizzare deve essere concordata precedentemente tra chi si scambia i messaggi e deve rimanere segreta tra i due.

Supponiamo che due persone vogliano scambiarsi questo messaggio:" assediare la città", (non è un caso che abbia scelto questa frase…. A quei tempi i messaggi cifrati erano utilizzati soprattutto tra militari per le operazioni di guerra).

Nel cifrario di Vigenere la chiave era un versetto, noi semplifichiamo ed usiamo una sola parola: "algebra".

La prima cosa da fare è scrivere la frase da cifrare senza spazi e nella riga sottostante ripetere la parola chiave fino ad esaurire la frase (attenzione: questo significa che si potrà ripetere la frase e l'ultima volta potrebbe anche essere incompleta, come nel nostro esempio):

ASSEDIARELACITTA

ALGEBRAALGEBRAAL

In questo modo ad ogni lettera del testo da cifrare viene associata una lettera della parola chiave. Scrivete adesso le corrispondenze in colonna in modo da facilitarvi il lavoro con la tavola di Vigenere.

A	A
S	L
S	
E	
D	
I	
A	
R	
E	
L	
A	
C	
I	
T	
T	
A	

La tavola sottostante invece crea una corrispondenza tra le lettere in chiaro e le lettere cifrate.

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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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 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

Si tratta di una sorta di schema di battaglia navale che in matematica prende il nome di matrice quadrata.

Il metodo da per cifrare è molto semplice: nella prima colonna si cerca la lettera da cifrare e nella prima riga la lettera associata alla parola chiave, all'incrocio tra le due cifre si trova la lettera cifrante:

esempio la prima lettera della frase da cifrare è A, la lettera corrispondente nella chiave è A e quindi rimane A, passiamo alla seconda è S a cui è associata la L di algebra, cerco S nella prima colonna, L nella prima colonna, all'incrocio trovo D, prendo la seconda S di assediare associata alla G di algebra, trovo la lettera Y e via di seguito.

Attività: completare la cifratura.

Secondo voi quali sono i punti deboli di questo cifrario? Fate le vostre considerazioni scrivendole in non più di dieci righe.