Szyfr Vigenere`a

Rodzaj: Polialfabetyczny szyfr podstawieniowy

Historia i zastosowanie: Słabość szyfrów monoalfabetycznych sprawiła, że próbowano wymyślać bardziej rozbudowane szyfry. Naturalnym krokiem było korzystanie z kilku alfabetów zamiast jednego jak w przypadku szyfrów monoalfabetycznych. Dało to początek polialfabetycznym szyfrom podstawieniowym. Idea takiego szyfru pojawiła się już w XV wieku (Leon Battista Alberti). Kolejne pomysły związane są z takimi nazwiskami jak Johannes Trithemius oraz Giovanni della Porta. W tym miejscu chciałbym przedstawić najbardziej znany szyfr polialfabetyczny stworzony przez Blaise de Vigenere`a, oficjalnie opublikowany w jego pracy "Traicte des Chiffres" w 1586 roku. Podczas tworzenia swojego szyfru Vigenere opierał się na przemyśleniach wcześniej wymienionych osób.

Opis metody: Tekst szyfrujemy na podstawie hasła. Szyfrowanie odbywa się w sposób następujący. Każdą literę tekstu jawnego szyfrujemy korzystając z alfabetu zaczynającego się od odpowiadającej litery w haśle. W przypadku, gdy hasło jest krótsze od szyfrowanego tekstu powtarzamy je wielokrotnie.
Szyfrowanie i deszyfrowanie odbywa się na podstawie tablicy Vigenere`a. Tablica Vigenere`a

Przykład:

Tekst jawny:	a	l	g	o	r	y	t	m	y	i	s	t	r	u	k	t	u	r	y	d	a	n	y	c	h
Hasło:	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v	i	g	e	n	e	r	e	v
Tekst zaszyfrowany	v	t	m	s	e	c	k	q	t	q	y	x	e	y	b	x	p	z	e	h	n	r	p	g	c

Jawny	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
	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

Opis procedury: Szyfrowany tekst znajduje się w pliku. Dodatkowo przed uruchomieniem procedury należy stworzyć drugi plik, będący plikiem wynikowym. W programie podajemy nazwy tych plików. Użytkownik podaje następnie hasło, korzystając jedynie z dużych liter z podstawowego alfabetu bez spacji i znaków interpunkcyjnych. Litery przepisywane są do tablicy hasło. Wartości ASCII tego hasła są przepisywane do tablicy tablica_ASCII (standardowo ustawiłem obie tablice na 200 elementów - jeżeli hasło byłoby dłuższe należy rozmiar ten w obu tablicach powiększyć). Gdy hasło jest krótsze następuje wartości wstawiane są od początku, aż zostanie wypełniona cała tablica. W przypadku gdy tekst jawny jest dłuższy niż 200 znaków należałoby również powiększyć obie wyżej wymienione tablice (w przypadku gdy byśmy tego nie zrobili korzystając z mojej procedury deszyfrującej odszyfrowanie powinno się powieść, jednak zostanie utracona ciągłość hasła i okres). Następnie otwierane są oba pliki i jeżeli operacja ta powiedzie się zaczyna się szyfrowanie. Za każdym razem pobierana jest jedna litera tekstu. Następnie według kod ASCII przydzielana jest ona do dwóch możliwych grup: duże lub małe litery. Wszystkie inne znaki w tym spacja podczas szyfrowania zostają usunięte. Każda pobrana litera jest następnie modyfikowana według odpowiadającej jej literze w haśle. Po zamianie każdej litery zapisywana jest ona w pliku wyjściowym. Na końcu oba pliki są zamykane i procedura kończy się.

Poziom bezpieczeństwa: Uzależniony od długości klucza. Od niskiego do bezwarunkowo bezpiecznego **one-time pad**