

Algorytmy podstawieniowe

Nazwa: AtBash

Rodzaj: Monoalfabetyczny szyfr podstawieniowy, ograniczony

Opis metody: Zasada jego działanie polega na podstawieniu zamiast jednej litery, litery leżącej po drugiej stronie alfabetu w takiej samej odległości od końca/początku. Najłatwiej będzie wyjaśnić to na przykładzie. Otóż za literę a powinniśmy podstawić literę z. Natomiast za literę c literę 3 od końca alfabetu a więc literę x. Warto zauważyć, że aby odszyfrować wiadomość należy ją ponownie zaszyfrować. Otrzymamy tym samym tekst jawny.

Przykład:

Tekst jawny: AlgorytmyiStrukturyDanych

Tekst zaszyfrowany: ZotlibgnbrHgifpgfibWzmbxs

Poziom bezpieczeństwa: Szyfr nie zapewnia bezpieczeństwa

Metody kryptoanalizy: Analiza częstości występowania poszczególnych liter w tekście.

Nazwa: Szyfr Cezara

Rodzaj: Monoalfabetyczny szyfr podstawieniowy, ograniczony

Historia i zastosowanie: Jest to szyfr za pomocą którego Juliusz Cezar szyfrował swoje listy do Cyserona. Jako ciekawostkę można podać, że szyfr ten był podobno używany jeszcze w 1915 roku w armii rosyjskiej, gdyż tylko tak prosty szyfr wydawał się zrozumiały dla sztabowców

Opis metody: Każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 3 miejsca w prawo. I tak literę A szyfrujemy jako literę D, literę B jako E itd. W przypadku litery Z wybieramy literę C. W celu odszyfrowania tekstu powtarzamy operację tym razem przesuwając litery o 3 pozycje w lewo.

Zapis matematyczny tych operacji wygląda następująco:

Szyfrowanie:

$$C=E(p)=(p+3)\bmod 26$$

Deszyfrowanie:

$$p=D(c)=(c-3)\bmod 26$$

Przyjmuje się, że alfabet składa się z 26 liter.

Przykład:

Tekst jawny: AlgorytmyiStrukturyDanych

Tekst zaszyfrowany: DojrubwpblVwuxnwxubGdqbfk

Poziom bezpieczeństwa: szyfr nie zapewnia bezpieczeństwa

Metody kryptoanalizy: analiza częstości występowania poszczególnych liter

Nazwa: ROT-13

Rodzaj: Monoalfabetyczny szyfr podstawieniowy, ograniczony.

Historia i zastosowanie: Algorytm ten używany był w grupach dyskusyjnych. Stosowanie jego nie miało jednak zapewnić tajemnicy. Szyfrowane były teksty często niecenzuralne tak, aby odczytywane były przez osoby, które sobie tego życzą. Dodatkowo zaszyfrowany tekst zawierający jakieś zabronione słowa przechodził bez problemu przez wszystkie filtry wyszukujące określonych wyrazów czy też fraz w tekstach. W późniejszym okresie filtry radziły sobie z tak prostym szyfrem.

Opis metody: Zasada działania jest identyczna jak w przypadku szyfru Cezara – różnica polega na wartości przesunięcia. W tym przypadku każdą literę tekstu jawnego zamieniamy na literę przesuniętą o 13 miejsca w prawo. W celu odszyfrowania tekst powtarzamy operację tym razem przesuwając litery o 13 pozycje w lewo.

Zapis matematyczny tych operacji wygląda następująco:

Szyfrowanie:

$$C=E(p)=(p+13)\bmod 26$$

Deszyfrowanie:

$$p=D(c)=(c-13)\bmod 26$$

Przyjmuje się, że alfabet składa się z 26 liter.

Należy również zauważyć, że przyjmując przesunięcie o wartości 13 przy deszyfrowaniu tekstu nie ważne jest czy wykonamy operację odejmowania czy dodawania (występuje przecież operacja mod 26). Zatem jeżeli szyfrujemy jedynie litery możemy użyć tej samej procedury do szyfrowania jak i deszyfrowania.

Poziom bezpieczeństwa: szyfr nie zapewnia bezpieczeństwa

Metody kryptoanalizy: analiza częstości występowania poszczególnych liter

Nazwa: 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: Szyfrowanie i deszyfrowanie odbywa się na podstawie tablicy Vigenere`a.

Tablica Vigenere'a

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

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 hasle. W przypadku, gdy hasło jest krótsze od szyfrowanego tekstu powtarzamy je wielokrotnie.

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
T. zaszyfrowany	W	U	N	T	F	D	L	R	U	R	Z	Y	F	Z	C	Y	Q	A	F	I	O	S	Q	H	D

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

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

Metody kryptoanalizy: Test Kasiskiego, indeks koincydencji.

Nazwa: Algorytm XOR

Rodzaj szyfru: Podstawieniowy

Historia i zastosowanie: Operacja ta jest częścią składową wielu rozbudowanych algorytmów kryptograficznych jak np. DES (Data Encryption Standard). Operacja ta sama w sobie stanowi również prosty algorytm szyfrowania, który nie zapewnia jednak większego bezpieczeństwa. Jednak przy spełnieniu kilku bardzo ważnych warunków może stanowić mimo swej prostoty algorytm niemożliwym do złamania (binarna wersja algorytmu one-time pad).

Opis metody: Oprócz tej nazwy możemy spotkać się z takimi nazwami jak alternatywa wykluczająca lub binarne sumowanie mod 2. W matematyce oznaczana jest często przez symbol krzyżyk w kółeczku. Operacja ta wygląda następująco:

$$0 \text{ XOR } 0 = 0$$

$$1 \text{ XOR } 1 = 0$$

$$0 \text{ XOR } 1 = 1$$

$$1 \text{ XOR } 0 = 1$$

Należy pamiętać, że w wyniku podwójnego wykonania operacji XOR otrzymamy tekst jawny. Zatem:

$$M \text{ XOR } K = C$$

$$C \text{ XOR } K = M$$

Czyli:

$$(M \text{ XOR } K) \text{ XOR } K = M$$

W wyniku tego mamy tylko jedną procedurę, zarówno do szyfrowania jak i do deszyfrowania.

Przykład:

Szyfrowanie

Tekst jawny: 0100 1010

Hasło: 0100 1000

Szyfrogram: 0000 0010

Deszyfrowanie

Szyfrogram: 0000 0010

Hasło: 0100 1000

Tekst jawny: 0100 1010

Poziom bezpieczeństwa:

- Dla krótkich kluczy – niski
- Dla kluczy długich (powyżej 160-bitów) – średni
- Przy spełnieniu pewnych warunków (one-time pad) – bezwarunkowo bezpieczny

Metody kryptoanalizy: Zliczanie koincydencji.

Nazwa: Szyfr One-time pad

Historia i zastosowanie: Jest to jedyny bezwarunkowo bezpieczny szyfr, co zostało udowodnione matematycznie w 1949 przez Shannon'a. Algorytm ten zaproponowany został przez Gilberta Vernama z AT&T w 1917 roku. Jeżeli chodzi o pojęcie klucza losowego to pierwszy raz wprowadził je Joseph Mauborgne.

W literaturze można spotkać informacje, że podobno gorąca linia pomiędzy Waszyngtonem a Moskwą szyfrowana była z wykorzystaniem tego algorytmu.

Opis metody: Można wyróżnić 2 wersje tego algorytmu:

- wersja binarna (szyfr Vernama)
- wersja znakowa (szyfr Vigenere'a)

W wersji binarnej szyfrujemy/deszyfrujemy korzystając z algorytmu Xor.

W wersji znakowej szyfrujemy/deszyfrujemy korzystając z algorytmu Vigenere'a.

Można zatem zadać sobie pytanie dlaczego tamte algorytmy zapewniają słabe lub średnie bezpieczeństwo a ten zapewnia bezwarunkowe bezpieczeństwo.

Otóż cała tajemnica tkwi tutaj w założeniach nałożonych na hasło.

Spełnione muszą być wszystkie 3 poniższe warunki:

- hasło musi być ciągiem losowym
- hasło musi być jednorazowe
- długość hasła musi być przynajmniej tak samo długa jak długość szyfrowanego tekstu

Przy krótkich tekstach nawet sprawdzenie wszystkich możliwości nie da nam odpowiedzi, gdyż napastnik otrzyma wiele poprawnych słów i nie będzie w stanie wybrać z nich słowa właściwego (bezpieczeństwo semantyczne).

Złamanie choćby jednego z tych warunków powoduje, że otrzymany szyfrogram może być już łatwy do odszyfrowania.

Jeżeli chodzi o 2 i 3 warunek to są one stosunkowo proste do spełnienia, chociaż trudno wyobrazić sobie przekazywanie nowego hasła dla każdej wiadomości.

Największym problemem jest wygenerowanie losowego hasła. Wiele metod, które mogą wydawać się losowe (stukanie w klawiaturę, ciąg wyliczany na podstawie czasu czy stanów procesora nie jest do końca wartością losową). Istnieją jednak algorytmy generujące ciągi pseudolosowe. Ciągi pseudolosowe są to ciągi generowane na podstawie losowego zarodka, korzystające z algorytmów deterministycznych. Powstający ciąg ma cechy ciągu losowego. Przykładowym algorytmem generującym ciągi pseudolosowe jest algorytm BBS.

Poziom bezpieczeństwo: Udowodniono bezwarunkowy poziom bezpieczeństwa

Metody kryptoanalizy: brak