Metody szyfrowania

Słownik pojęć

- Tekst jawny (tekst otwarty) - wiadomość, która nie została jeszcze zaszyfrowana
- Szyfrogram (kryptogram) - wiadomość, która została zaszyfrowana

Szyfry klasyczne

Podział

- Szyfry podstawieniowe - każda litera tekstu jawnego zostaje zastąpiona innym, ustalonym wcześniej znakiem
- Szyfry przestawieniowe - tworzone poprzez przestawienie kolejności znaków w tekście jawnym
- Szyfry mieszane - połączenie szyfru podstawieniowego z przestawieniowym

Szyfry podstawieniowe

Podział

- Szyfry monoalfabetyczne - każdemu znakowi alfabetu jawnego przyporządkowywany jest jeden znak alfabetu tajnego
- Szyfry homofoniczne - każdemu znakowi alfabetu jawnego przyporządkowywana jest grupa znaków alfabetu tajnego
- Szyfry polialfabetyczne - używanych jest wiele alfabetów tajnych, które służą do kodowania poszczególnych znaków tekstu jawnego
- Szyfry poligramowe - szyfrowane są grupy znaków

Szyfr Cezara

- Alfabet wykorzystywany do szyfrowania jest przesunięty o 3 pozycje w prawo względem oryginalnego

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
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

Szyfr AtBash

- Szyfr monoalfabetyczny wywodzący się z tradycji żydowskiej
- Zamiast każdej z liter alfabetu jawnego podstawia się literę, która leży w takiej samej odległości od końca alfabetu, co dana litera od początku
- W praktyce polega na odwróceniu alfabetu

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

Szyfr książkowy

- Przykład szyfru homofonicznego
- Zamiast litery podstawiamy trzy liczby - nr strony, nr wiersza i nr znaku
- Szyfrowanie i deszyfrowanie odbywa się na podstawie ustalonej książki

Szyfr Playfaira

- Szyfr monoalfabetyczny
- Opiera się na tabeli 5x5 utworzonej ze wszystkich litera alfabetu.
- Literę I i J stosuje się zamiennie.

Szyfr Playfaira - tworzenie tabeli

- Tworzymy tabelę 5x5
- W początkowe komórki wpisujemy litery klucza (bez powtórzeń)
- Uzupełniamy pozostałymi literami alfabetu

Przykład

- Klucz: MAGISTER

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

Szyfr Playfaira - szyfrowanie

- Tekst jawny dzielimy na dwuznaki
- Każde dwa znaki, oddzielnie, znajdujemy w tabeli i zaznaczamy prostokąt utworzony przez te litery
- Szyfrogramem dla danego dwuznaku są litery leżące na pozostałych rogach prostokąta

Przykład

- Dwuznak: ST
- Szyfrogram: MC

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

Przypadki szczególne

- Jeżeli litery leżą w tej samej kolumnie, odczytujemy z wiersza poniżej
- Dwuznak: CU; Szyfrogram: LZ

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

Przypadki szczególne

- Jeżeli litery leżą w tym samym wierszu, odczytujemy litery z prawej strony
- Dwuznak: PO; Szyfrogram: QP

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

Przypadki szczególne

- Jeżeli litera leży w ostatniej kolumnie, odczytuje się litery z pierwszej kolumny
- Jeżeli litera leży w ostatnim wierszu, odczytuje się litery z pierwszego wiersza
- Jeżeli tekst składa się z nieparzystej liczby liter, dopisuje się literę X