Temat lekcji: Wprowadzenie do kryptografii

Klasa: II LO

Ilość godzin: 2

Cele ogólne:

Zapoznanie ucznia z terminem kryptografii i rodzajami szyfrów i uświadomienie uczniom roli kodowania w przesyłaniu danych np. dostęp do stron internetowych banków.

Metody: elementy wykładu, dyskusja, ćwiczenia i praktyczne działanie

Środki dydaktyczne: tablica, karty ćwiczeń

Przebieg lekcji:

I. Sprawy organizacyjne:

a. Lista obecności
b. Sprawdzenie wiadomości z ostatniej lekcji

II. Podanie tematu i uświadomienie celu

III. Treść lekcji

Wykład:

Kryptografia to sztuka ochrony danych w taki sposób, aby tylko powołana osoba mogła je odczytać. Jest to realizowane za pomocą szyfrowania (encryption). Zaszyfrowany tekst w języku angielskim - nazywa się ciphertext. Proces odwrotny do szyfrowania to deszyfracja (decryption).

Kryptoanaliza to z kolei sztuka czytania zaszyfrowanych wiadomości bez posiadania odpowiednich uprawnień (klucza, algorytmu). Kryptoanaliza to nic innego jak łamanie szyfrów.

Kryptologia to połączenie kryptografii i kryptoanalizy.

Informacja zaszyfrowana to zwykła informacja (tzw. jawna) przetworzona przez funkcję szyfrująca do postaci nieczytelnej. Tylko osoba dysponująca właściwą funkcją szyfrującą może przetworzyć tą informację do czytelnej postaci.

Funkcja szyfrująca przetwarza informacje (jawną) na nieczytelną (zaszyfrowaną).

Funkcja deszyfrująca przetwarza informację zaszyfrowaną (nieczytelną) na jawną (odszyfrowaną).

Tekst jawny może być ciągiem bitów, plikiem tekstowym, ciągiem próbek głosu lub cyfrowym obrazem wideo. Dla komputerów to po prostu dane binarne. Tekst ten może być przeznaczony do przesyłania lub do zapamiętania. W każdym przypadku jest wiadomością do zaszyfrowania.

Rozróżniamy dwa podstawowe rodzaje szyfrów: **przestawieniowe i podstawieniowe**. Szyfry przestawieniowe zmienjają uporządkowanie bitów lub znaków w danych. W szyfrach podstawieniowych bity, znaki lub bloki znaków są zastępowane ich ustalonymi zamiennikami.

Przykłady szyfrów przestawieniowych (permutacyjnych).

1. Przy tzw. przestawieniu kolumnowym tekst jawny zapisuje się do macierzy wierszami. Tekst zaszyfrowany powstaje przez odczyt kolumnami w określonym porządku.

Przykład: Mam tekst jawny METAMORFOZA zapisuje go wierszami w macierzy o wymiarach 3 x 4

1	2	3	4
M	E	T	A
M	O	R	F
O	Z	A	

Przy odczycie kolumn w kolejności 2-4-1-3 tekst zaszyfrowany będzie miał postać EOZAFMMOTRA.

2. Wiele szyfrów przestawieniowych zmienia kolejność znaków tekstu jawnego przy zastosowaniu *stałego okresu d*. Zakładam, że d = 4, f zaś jest permutacją:

i:	1	2	3	4
f(i):	2	4	1	3

tak więc pierwszy znak tekstu jawnego jest przesunięty na trzecią pozycję w tekście zaszyfrowanym, drugi znak tekstu jawnego znajdzie się na pierwszej pozycji i tak dalej. Tekst jawny METAMORFOZA zostanie zaszyfrowany jako:

M = META MORF OZA

E_k(M)= EAMT OFMR ZOA

Przykłady szyfrów podstawieniowych

Istnieją cztery typy szyfrów podstawieniowych: monoalfabetyczne, homofoniczne, wieloalfabetyczne i poligramowe. Szyfry monoalfabetyczne zamieniają każdy znak tekstu jawnego na odpowiedni znak kryptogramu, przy czym w całej wiadomości do zamiany każdego znaku jawnego na zaszyfrowany stosuje się odwzorowanie „jeden do jednego". Szyfry homofoniczne są podobne z tym wyjątkiem, że odwzorowanie ma charakter „jeden do wielu" i każdy znak tekstu jawnego może być zaszyfrowany jako jeden z pewnej grupy znaków alfabetu szyfrowego. W szyfrach wieloalfabetycznych stosuje się wiele odwzorowań znaków tekstu jawnego na znaki tekstu zaszyfrowanego, przy czym każde odwzorowanie jest zazwyczaj typu „jeden do jednego", podobnie jak w szyfrach monoalfabetycznych. Szyfry poligramowe są najbardziej ogólną metodą, umożliwiającą dowolne podstawienia za grupy znaków.

1. Funkcja f odwzorowuje alfabet angielski $\aleph$ = {A, B, ..., Z} w taki oto alfabet zaszyfrowany (nazwa szyfru simple substitution):

$\aleph$: 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

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

Wtedy tekst jawny METAMORFOZA zostaje zaszyfrowany jako: GSTHGKNIKZH

W podanym przykładzie użyto alfabetu mieszanego wg klucza: alfabet szyfru powstaje z liter słowa kluczowego (w tym przypadku HARPSICHORD) z eliminacją powtórzeń oraz pozostałych kolejnych liter alfabetu.

2. Szyfry oparte na alfabetach przesuniętych przesuwają litery alfabetu w prawo o k pozycji modulo wielkość alfabetu. Formalnym zapisem tego typu alfabetu będzie wzór

$$f(a) = (a+k) \bmod n$$

przy czym n jest licznością alfabetu **א**, zaś a oznacza literę alfabetu **א**, jak i jego pozycję w **א**. Dla alfabetu angielskiego n = 26. Poszczególne litery mają w nim następujące pozycje:

0 - A, 1 - B, 2 - C, 3 - D, 4 - E, ..., 20 - U, 21 - V, 22 - W, 23 - X, 24 - Y, 25 - Z.

Ten rodzaj szyfru jest nazywany szyfrem Cezara, gdyż jako pierwszy użył go Juliusz Cezar dla k=3. Nasz tekst jawny RENAISSANCE zaszyfrowany szyfrem Cezara ma postać: UHQDLVVDQFH.

3. Szyfr homofoniczny odwzorowuje każdy znak a alfabetu tekstu jawnego na zestaw elementów *f*(a) tekstu zaszyfrowanego, zwanych homofonami. Zakładam, że litery alfabetu angielskiego są szyfrowane jako liczby całkowite z przedziału (0, 99), przy czym ilość liczb całkowitych przydzielonych danej literze jest proporcjonalna do względnej częstości jej występowania i żadna z tych liczb nie jest przydzielona do więcej niż jednej litery.

Podam teraz możliwy przydział liczb do liter w wiadomości o treści PLAIN PILOT

Litera	Homofony
A	17 19 34 41 56 60 67 83
I	08 22 53 65 88 90
L	03 44 76
N	02 09 15 27 32 40 59
O	01 11 23 28 42 54 70 80
P	33 91
T	05 10 20 29 45 58 64 78 99

Jedną z możliwych postaci zaszyfrowania podanego komunikatu jest:

M = P L A I N P I L O T

C = 91 44 56 65 59 33 08 76 28 78

Podać przykładowy przydział liczb dla zdania Informatyka dla liceum ogolnoksztalcacego. Pokazać dwie możliwości zakodowania tego zdania.

4. Szyfr Vigenere

Szyfr Vigenere jest szyfrem podstawieniowym wieloalfabetycznym. Algorytm ten oparty jest na tablicy przedstawionej poniżej:

	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**	**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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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	Z	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
Z	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	Z
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	Z	Y

Szyfr ten wymaga klucza, tekst zakodowany powstaje poprzez napisanie klucza pod tekstem jawnym. W następującym przykładzie jako tekst jawny posłużmy się słowem KRYPTOGRAFIA a klucz to słowo SZYFR.

Tekst do kodowania: K R Y P T O G R A F I A

Klucz: S Z Y F R S Z Y F R S Z

Aby otrzymać tekst zakodowany prześledźmy następujące rozważania, pierwszym krokiem jest użycie tablicy Vigenere'a. Bierzemy pod uwagę pierwszą literę tekstu do kodowania - K i znajdujemy jej położenie w pierwszym wierszu tablicy, następnie bierzemy pierwszą literę klucza - S i znajdujemy jej położenie w pierwszej kolumnie tablicy, na przecięciu znalezionego wiersza i kolumny znajduje się pierwsza litera tekstu zakodowanego. Kontynuujemy w ten sam sposób do momentu aż skończy się cały tekst do kodowania.

Tekst do kodowania: K R Y P T O G R A F I A

Klucz: S Z Y F R S Z Y F R S Z

Tekst zakodowany: D Q Y V L H F R G X B Y

Jak łatwo zauważyć te same litery w tekście jawnym nie zostały zakodowane na te same w kodzie np.: litera A została zakodowana jako G a następnie jako Y, jest to ważna cecha szyfrów wieloalfabetycznych, która utrudnia kryptoanalizę.

Odkodowanie jest proste jeżeli znamy klucz, bierzemy pierwszą literę klucza i po znalezieniu jej w pierwszej kolumnie sprawdzamy w wierszu wyznaczonym przez nią gdzie znajduje się początkowa litera tekstu zakodowanego. Następnie odczytujemy literę znajdującą się w pierwszym wierszu w kolumnie wyznaczonej przez literę zakodowaną - jest to litera teksu jawnego.

5. Szyfr Playfair

Szyfr Playfair'a jest digramowym szyfrem podstawieniowym. Kluczem do tego szyfru jest macierz o wymiarach 5 x 5 składająca się z liter (litera J nie była używana). Każdą parę liter tekstu jawnego m_1m_2 szyfruje się według następujących reguł:

1. Jeśli m_1 i m_2 znajdują się w tym samym wierszu, to c_1 i c_2 są znakami z prawej strony m_1 m_2, przy czym pierwszą kolumnę traktuje się jako położoną na prawo od ostatniej kolumny.

2. Jeśli m_1 i m_2 znajdują się w tej samej kolumnie, to c_1 i c_2 są znakami położonymi poniżej m_1 i m_2, przy czym pierwszy wiersz traktuje się jako leżący pod ostatnim wierszem.

3. Jeśli m_1 i m_2 znajdują się w różnych wierszach i kolumnach, to c_1 i c_2 są brane z przeciwległych rogów prostokąta wyznaczonego przez m_1 i m_2, przy czym c_1 pochodzi z wiersza zawierającego m_1, c_2 zaś - z wiersza zawierającego m_2.

4. Jeśli $m_1 = m_2$, to do tekstu jawnego między te litery wstawia się nieznaczącą literę (np. X), co eliminuje powtórzenia.

5. Jeśli tekst jawny ma nieparzystą liczbę znaków, to na końcu tekstu jawnego dopisuje się nieznaczącą literę.

H A R P S

I C O D B

E F G K L

M N Q T U

V W X Y Z

Przykład: Szyfruję słowo METAMORFOZA, korzystam z macierzy przedstawionej powyżej

ME TA MO RF OZ AX

VM NP QI AG BX RW

Zadanie:

Zakoduj następujące słowa:

Szyfr	Igrupa	II grupa	III grupa	IV grupa
Przestawieniowy 1	pseudojezyk, konfigurowanie	Inzynieria, parasol	przetwarzanie, zmiennopozycyjna	Software, statek
Przestawieniowy 2	przetwarzanie, zmiennopozycyjna	Oprogramowanie, wersalka	pseudojezyk, konfigurowanie	Hardware, wedkarstwo
Podstawieniowy 1	Utworzyć alfabet według klucza: formularz i zakodować słowa: struktura, przesdsiebiorstwo.	Utworzyć alfabet według słowa: malarz i zakodować słowa: statek, wedkarstwo	Utworzyć alfabet według klucza domek i zakodować słowa: gladiator, mucha.	Utworzyć alfabet według słowa: telefon i zakodować słowa: parasol, wersalka
Podsatwieniowy 2	telewizja, poranek	Listopad, drzwi	wrzesien, pazdziernik	Raport, kwerenda
Hmofoniczny	Podać przykładowy przydział liczb dla zdania Informatyka dla liceum ogolnoksztalcacego. Pokazać dwie możliwości zakodowania tego zdania.	Podać przykładowy przydział liczb dla wyrażenia: struktura programu. Pokazać dwie możliwości zakodowania tego wyrażenia.	Podać przykładowy przydział liczb dla wyrażenia: Algorytmy iteracyjne. Pokazać dwie możliwości zakodowania tego wyrażenia.	Podać przykładowy przydział liczb dla wyrażenia: Meandry języka. Pokazać dwie możliwości zakodowania tego wyrażenia.
Vigenere	Zakodować słowa: gladiator, mucha z kluczem: domek	Zakodować słowa: informatyka, pustynia z kluczem okno	Zakodować słowa: struktura, przesdsiebiorstwo z kluczem formularz.	Zakodować słowa: klawiatura, krzeslo z kluczem niebo.
Playfair	wrzesien, pazdziernik	Raport, kwerenda	telewizja, poranek	Listopad, drzwi

Podsumowanie zajęć.

- Pogadanka na temat konieczności kodowania danych na stronach internetowych
- Pytania sprawdzające
- Ocena uczniów za udział w lekcji