Uniwersytet Bielsko-Bialski

Wydział Budowy Maszyn i Informatyki

CYBERBEZPIECZEŃSTWO
(ćwiczenia projektowe №4)

Temat ćwiczenia: Licencji oprogramowania komputerowego

1. Wprowadzenie

W klasycznym modelu rozpowszechniania programów komputerowych, korzystanie z nich odbywa się na podstawie odpłatnej licencji oprogramowania.

Licencja oprogramowania – umowa na korzystanie z utworu, jakim jest aplikacja komputerowa, zawierana pomiędzy podmiotem, któremu przysługują majątkowe prawa autorskie do utworu, a osobą, która zamierza z danej aplikacji korzystać.

Użytkownicy komputerów najczęściej mogą spotykać się z licencją w odniesieniu do tzw. **licencji użytkownika (EULA)**, które są używane przez producentów oprogramowania do wiązania użytkowników dodatkowymi ograniczeniami.

Licencje na oprogramowanie są najczęściej bardzo restrykcyjne i większość użytkowników nie czyta ich w ogóle. Większość takich licencji ogranicza liczbę komputerów, na których można zainstalować oprogramowanie, liczbę użytkowników, którzy mogą go używać i wprowadzają wiele innych ograniczeń, które nie są bezpośrednio związane z technologią.

Rodzaje licencji oprogramowania komputerowego:

- **Freeware** – licencja oprogramowania umożliwiająca darmowe rozprowadzanie aplikacji bez ujawnienia kodu źródłowego. Czasami licencja freeware zawiera dodatkowe ograniczenia (np. część freeware jest całkowicie darmowa jedynie do użytku domowego).
- **Shareware** – rodzaj oprogramowania zamkniętego, które jest bezpłatnie rozpowszechniane i którego kopiami wolno się dzielić, jednak korzystanie z jego pełnej funkcjonalności wymaga wniesienia określonych opłat po pewnym okresie użytkowania lub zakupu licencji.
- **Adware** – jest oprogramowaniem rozpowszechnianym za darmo, którego producent otrzymuje wynagrodzenie za wyświetlanie reklam zlecanych przez sponsorów.
- **Trialware** – rodzaj licencji na programy komputerowe polegający na tym, że można go używać przez z góry ustalony czas (od 7 do 90 dni). Czasami zamiast ograniczenia na liczbę dni jest ograniczenie na liczbę uruchomień programu. Programy na tej licencji są w pełni funkcjonalne. Po upływie ustalonego czasu, zgodnie z licencją, wymagane jest uzyskanie wersji pełnej programu albo usunięcie go z dysku twardego. Większość tego typu programów po upływie tego czasu blokuje działanie części lub całości funkcjonalności do czasu zakupienia pełnej licencji i wprowadzenia klucza odblokowującego.
- **Demoware** – wersja zwykle komercyjnego programu komputerowego. Zazwyczaj jest to wersja o ograniczonej funkcjonalności w stosunku do wersji pełnej lub wersja pełna o ograniczonej czasowo możliwości wykorzystania. W przypadku gier komputerowych jest to zwykle jeden poziom z finalnej produkcji.

Klucze odblokowujące ograniczenia oprogramowania według licencji są często szyfrowane. Rozważmy dwa tradycyjne algorytmy szyfrowania: szyfr Cezara oraz szyfr Vigenere'a.

Szyfr Cezara jest jednym z najstarszych sposobów szyfrowania. Juliusz Cezar szyfrował tym sposobem swoje wiadomości do Cycerona. Jest to jedna z najprostszych technik szyfrowania. Jest to szyfr podstawieniowy, w którym każdą literę tekstu niezaszyfrowanego zastępujemy oddaloną od niej o stałą liczbę pozycji w alfabecie inną literą, przy czym musimy zachować kierunek zmiany.

Każdą literę w alfabecie zastępujemy inną literą znajdującą się trzy miejsca dalej.

A	B	C	D	E	F	G	H	I	J	K	L	M
D	E	F	G	H	I	J	K	L	M	N	O	P

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Szyfr Vigenère'a jest wieloalfabetowym szyfrem podstawieniowym. Polega więc na stosowaniu różnie zdefiniowanych podstawień dla kolejnych liter tekstu. W przeciwieństwie do niektórych szyfrów wieloalfabetowych, strony nie muszą zapamiętywać i wymieniać pomiędzy sobą wszystkich zdefiniowanych przekształceń liter alfabetu. Użyte rozwiązanie redukuje ilość informacji, które trzeba zapamiętać do zaledwie jednego sekrentego słowa (lub zdania).

Do szyfrowania i odkodowywania wykorzystuje się tablicę zawierającą w pierwszym wierszu litery alfabetu w oryginalnej kolejności, a następnie w każdym kolejnym wierszu litery alfabetu przesunięte o jedną kolejną pozycję w lewo. Tablica ta nosi łacińską nazwę tabula recta i została po raz pierwszy używa w kryptografii przez niemieckiego mnicha Johannes Trithemius.

	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
A	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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	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

Tabula Recta

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

2. Zadanie do zrealizowania:

Udoskonal program utworzony w ćwiczeniu 3, który wprowadza licencje na oprogramowanie oraz implementuje następujące zasady dla systemu bezpieczeństwa:

1. Dodaj funkcję nakładające ograniczenia użytkowania programu według zadania indywidualnego.
2. Zrealizuj algorytm szyfrujący i deszyfrujący dla klucza odblokowującego funkcję ograniczenia użytkowania programu według zadania indywidualnego.

3. Zadania indywidualne

№	Rodzaje licencji	Funkcję	Ograniczenia	Algorytm
1	Demoware	Otwieranie plików	Rozmiar otwieranych plików nie przekracza 100 KB	Szyfr Cezara
2	Demoware	Otwieranie plików	Otwieranie plików tylko w formacie TXT	Szyfr Vigenere'a
3	Demoware	Zapisywanie plików	Blockowanie zapisywania plików	Szyfr Cezara
4	Demoware	Drukowanie	Blockowanie funkcji drukowania	Szyfr Vigenere'a
5	Trialware	Edytowania plików	Ograniczenie na liczbę uruchomień programu (5 raz)	Szyfr Cezara

6	Trialware	Wyświetlanie plików	Blokowanie funkcji na koniec bieżącego miesiąca	Szyfr Vigenere'a
7	Trialware	Otwieranie plików	Blokowanie programu w 19:00 godz.	Szyfr Cezara
8	Nagware	Zapisywanie plików	Okno dialogowe przypominające o zarejestrowaniu programu po każdych 5 minutach pracy	Szyfr Vigenere'a
9	Nagware	Drukowanie	Okno dialogowe przypomnienia o rejestracji programu po każdym uruchomieniu programu	Szyfr Cezara
10	Nagware	Edytowania plików	Podczas otwierania programu uruchom przeglądarkę na stronie google	Szyfr Vigenere'a