Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных машин

Дисциплина: Защита информации в информационных системах

ОТЧЕТ
по практической работе № 3
на тему
«Шифрование»

Студент:

Преподаватель:

МИНСК 2024

1 ЦЕЛЬ РАБОТЫ

Изучить различные виды шифрования.

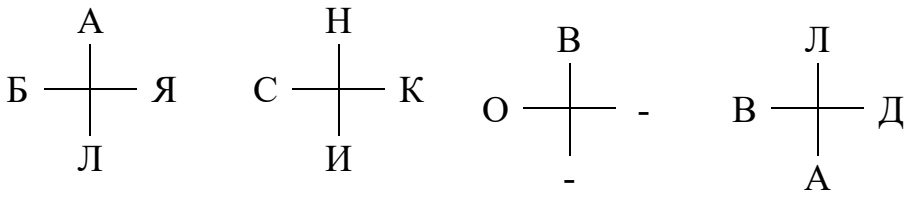
2 ВЫПОЛНЕНИЕ РАБОТЫ

2.1 Методы шифрования с перестановками

1. Перечислить методы шифрования с перестановками

Простая одинарная перестановка, блочная одинарная перестановка, табличная маршрутная перестановка, вертикальная перестановка, «Перекресток», «Поворотная решетка», магический квадрат, двойной перестановки.

2. Шифрование имени и фамилии шифром «Перекресток» (N=2).



БАЛЯСНИКОВ ВЛАД – «АНВБЯСКО ЛИ ЛВДА»

Для расшифровки нужно в соответствии с оговорённым количеством букв расставить их в соответствующие строки. Затем согласно алгоритму расстановки расшифровать сообщение.

Пример:

Расшифровать «еоисвилткаио» (N=3).

	е	
с		В
	а	

	о	
п		Л
	и	

	и	
т		К
	о	

Результат севаполитико

3. Шифрование имени и фамилии шифром двойной перестановки.

	4	1	3	2
3	Б	А	Л	Я
1	С	Н	И	К
4	О	В	+	В
2	Л	А	Д	_

	1	2	3	4
3	А	Я	Л	Б
1	Н	К	И	С
4	В	В	+	О
2	А	_	Д	Л

	1	2	3	4
1	Н	К	И	С
2	А	_	Д	Л
3	А	Я	Л	Б
4	В	В	+	О

Балясников Влад - «НКИСА_ДЛАЯЛБВВ+О»

Для расшифровки сообщения необходимо знать размеры таблицы, маршруты вписывания и выписывания, а также порядки перестановки столбцов и строк.

Пример:

Расшифровать «оиеиоалквптс».

	1	2	3	4
1	о	и	л	п
2	и	о	к	т
3	е	а	в	с

	1	2	3	4			4	1	3	2
3	е	а	в	с		3	с	е	в	а
1	о	и	л	п		1	п	о	л	и
2	и	о	к	т		2	т	и	к	о

Результат: севаполитико

2.2 Методы шифрования с заменами

1. Перечислить методы шифрования с заменами.

1) Регулярные шифры однозначной замены (Шифр Цезаря, атбаш, лозунговый шифр, полибианский квадрат, тюремный шифр, шифрующая система Трисемуса(Тритемия), шифр масонов);

2) Полиграммные шифры (биграммный шифр Порты, шифр «Честная игра», шифр Хилла);

3) Нерегулярные шифры (совмещённый шифр);

4) Омофонические шифры(система омофонов, книжный шифр, вариантные шифры);

5) Полиалфавитные шифры (диск Альберти, таблица Трисемуса, система шифрования Виженера, роторные машины, шифры Тени).

2. Шифрование имени и фамилии шифром Цезаря (ключ=5).

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д

Балясников Влад– «Ёердцтнпуж Жреи»

Для расшифровки сообщения необходимо знать ключ.
Пример: «Фсег Тсолхлнс» (ключ=4)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Результат: Сева Политико

3. Шифрование имени и фамилии биграммным шифром Порты.

	А	Б	В	Г	Д	Е (Ё)	Ж	З	И (Й)	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	001	002	003	004	005	006	007	008	009	010	011	012	013	014	015	016	017	018	019	020	021	022	023	024	025	026	027	028	029	030	031
Б	032	033	034	035	036	037	038	039	040	041	042	043	044	045	046	047	048	049	050	051	052	053	054	055	056	057	058	059	060	061	062
В	063	064	065	066	067	068	069	070	071	072	073	074	075	076	077	078	079	080	081	082	083	084	085	086	087	088	089	090	091	092	093
Г	094	095	096	097	098	099	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124
Д	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155
Е (Ё)	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186
Ж	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217
З	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248
И (Й)	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279
К	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310
Л	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341
М	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372
Н	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403
О	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434
П	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465
Р	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496
С	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523	524	525	526	527
Т	528	529	530	531	532	533	534	535	536	537	538	539	540	541	542	543	544	545	546	547	548	549	550	551	552	553	554	555	556	557	558
У	559	560	561	562	563	564	565	566	567	568	569	570	571	572	573	574	575	576	577	578	579	580	581	582	583	584	585	586	587	588	589
Ф	590	591	592	593	594	595	596	597	598	599	600	601	602	603	604	605	606	607	608	609	610	611	612	613	614	615	616	617	618	619	620
Х	621	622	623	624	625	626	627	628	629	630	631	632	633	634	635	636	637	638	639	640	641	642	643	644	645	646	647	648	649	650	651
Ц	652	653	654	655	656	657	658	659	660	661	662	663	664	665	666	667	668	669	670	671	672	673	674	675	676	677	678	679	680	681	682
Ч	683	684	685	686	687	688	689	690	691	692	693	694	695	696	697	698	699	700	701	702	703	704	705	706	707	708	709	710	711	712	713
Ш	714	715	716	717	718	719	720	721	722	723	724	725	726	727	728	729	730	731	732	733	734	735	736	737	738	739	740	741	742	743	744
Щ	745	746	747	748	749	750	751	752	753	754	755	756	757	758	759	760	761	762	763	764	765	766	767	768	769	770	771	772	773	774	775
Ъ	776	777	778	779	780	781	782	783	784	785	786	787	788	789	790	791	792	793	794	795	796	797	798	799	800	801	802	803	804	805	806
Ы	807	808	809	810	811	812	813	814	815	816	817	818	819	820	821	822	823	824	825	826	827	828	829	830	831	832	833	834	835	836	837
Ь	838	839	840	841	842	843	844	845	846	847	848	849	850	851	852	853	854	855	856	857	858	859	860	861	862	863	864	865	866	867	868
Э	869	870	871	872	873	874	875	876	877	878	879	880	881	882	883	884	885	886	887	888	889	890	891	892	893	894	895	896	897	898	899
Ю	900	901	902	903	904	905	906	907	908	909	910	911	912	913	914	915	916	917	918	919	920	921	922	923	924	925	926	927	928	929	930
Я	931	932	933	934	935	936	937	938	939	940	941	942	943	944	945	946	947	948	949	950	951	952	953	954	955	956	957	958	959	960	961

Ба ля сн ик ов Вл ад- «002 941 389 288 076 313 125»

Для расшифровки сообщения необходимо знать таблицу шифрозамен.

Пример:
Расшифровать «502 063 448 319 536 293»

Результат «СЕ ВА ПО ЛИ ТИ КО»

3.1 Комбинированные шифры

1. Сети Фейстеля

Сеть Фейстеля состоит из нескольких ячеек. На определенном раунде шифрования шифруемый блок разбивается на две равные половинки - H_i (высший, high) и L_i (низкий, low). К правой половинке применяется функция шифрования f с использованием ключевого элемента k_i (части ключа или модификации части ключа). После этого выполняется сложение по модулю два левой половинки и результата модификации правой половинки. В результате шифруемым блоком для следующего раунда будет объединение половинок, полученных по формулам

$$H_{i+1} = L_i, \quad (1)$$

$$L_{i+1} = Hi \oplus f(L_i, k_i). \quad (2)$$

2. Режимы DES

электронная кодовая книга ECB (Electronic Code Book)
сцепление блоков шифра CBC (Cipher Block Chaining)
обратная связь по шифротексту CFB (Cipher Feed Back)
обратная связь по выходу OFB (Output Feed Back)

3. Операции с данными (методы шифрования)

замена - функция расширения E, узлы замены S;
перестановка – перестановки IP, IP-1 , P, PC1, PC2, чередование Li и Hi, циклический сдвиг;
гаммирование – $\oplus$.

4. Длина блока

64 бит.

5. Длина ключа

64 бит.

6. Шифрование имени и фамилии шифром ADFGVX

	A	D	F	G	V	X
A	Ю	У	И	Ч	К	Б
D	В	Г	Е	Ф	Ж	З
F	Й	А	Л	М	О	П
G	Р	Щ	Т	Я	Ё	Х
V	Ц	Н	Ш	С	Ъ	Ы
X	Ь	Э	Д	-	-	-

Набор шифрозамен: Балясников Влад - «AX FD FF GG VG VD AF AV FV DA DA FF FD XF»

Ключевое слово: ЗАМЕНА

З	A	M	E	H	A
4	1	5	3	6	2
V	G	F	D	V	A
A	D	G	F	F	D
A	V	A	F	G	A
A	F	F	F	F	F

Окончательная шифрограмма: «GDVFA DAFDF FFVAA AFGAF VFGF»

Для расшифровки сообщения необходимо знать таблицу шифрозамен и ключевое слово.

Пример:

Расшифровать «AVDFD GDF» (ключевое слово – политико)

п	о	л	и	т	и	к	о
2	6	3	4	5	1	8	7
V	G	D	F	D	A	F	D

«VG DF DA FD»

Результат: сева

3 ВЫВОД

Изучил шифры «Перекрёсток», двойной перестановки, Цезаря, биграммный шифр Порты, ADFGVX.