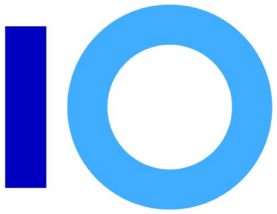

"Ss. Cyril and Methodius" University in Skopje
FACULTY OF COMPUTER
SCIENCE AND ENGINEERING

Лабораториска вежба бр. 1 по предметот

"Криптографија"

Substitution cryptography

Изработил:

Мартин Костадинов

Број на индекс:

161159

ВОВЕД

Во оваа документација ќе биде прикажан начинот на кој е дешифрирана пораката добиена од професорот задолжен за спроведување на вежбите по предметот “Криптографија”.

Пораката добиена изгледа вака:

НШГЖИЛЏЛЈЛВШЃSHJЧЗШЛЃТГЃSШЖГЃЃГJЗЏБЖЛЏЧФГJЃSAЏSЏЧФЛСJНЃSГЃСJФГJЏБЏЏНJЧЗЃЧШSСЧВJФSJСШSШВШГJSJЛВШJФSJСШКЏSШНШГЖИЛЏЛВШ
ЃSHJЧЗШЛЃТГЃSШЖГЃЃГJЗЏБЖЛЏЧФГJЃSAЏSЏЧФЛСJСJФJФЛШСSШЖSЃСЏЧВЃЛЏЛJЛФСГЃЧЃИЃЗЏЛJЌЃБФГJЏБЏJРБШСЏSСJФИЖАРЏSСЏФSЃГSШЧЗВШГJ
SJЛФЛШЏЃSШФЃИШSШФЏЌЗЃБШSЖШЧЃЌСЏЃИБШЌЃЃЏЌЃSШЏФЏЛЛШУJЌЃSШНШГЖИЛЏЛJЛВШЃSHJЧЗШЛЃТГЃSШЖГЃЃГJЗЏБЖЛЏЧФГJЃSAЏSЏЧФЛСJНЃSГЃЏЧ
ЏВЖИЛШЛSШВЌЧЖАЖСШКЏЛJSШЌСШЛШSШБУJИЏЗЃЃSФЛЃЛЖЛЃJЌJРИШФЛШSШЃSHJЧЗШЛЃГШЛШЃГJЗЏБЖЛЏЧФГШЛШЛЏЊSЃГШСJЗШГЏЌJSЃБШЃSФЛЃЛЖЛJЛВ
ШЃSHJЧЗШЛЃГШЃГЏЃЧЃЏЧЃЧJЌSJЗШЛЏЗШЛЃТГЃJЛНШГЖИЛЏЛЃЃSФЛЃЛЖЛJЛВШГJЗЏБЖЛЏЧФГШЛЏЊSЃГШЃГSHJЧЗШЛЃГШЃГЛЃЏЧЃНШГЖИЛЏЛJЛВШЏИЏГЛЧ
JЛЏЊSЃГШЃГSHJЧЗШМЃФГЃЛЏЊSJИJУГЃЃСJЌШЌЏSШЛШНJЧЗШЌСШЛШЃSФЛЃЛЖЛЃЧШРJЛШЛЖПЛЏJЌJФЖЗЌЏФЏЛЛЃЛЏУJЌЃSГSШЗГSШЛЃJЛСЏГЃЃЏJТSЖСШЌ
ШЧШРJЛЃJЌЌШИЏTSШЛШJФЖЗЌЏФЏЛЃЏЏЛЛШУJЌГSШГШГJЧШЗSJЏЧШСSШФJФЛШСSШМЏИЃSШSШЏJСЛJЧSJJРЏЌГSЏЛГJЛЏЗНЏJЌГЗЏЛJГSФЛЃЛЖЛВШГSHJЧ
ЗШЛГШГГЛЃЏJЛЏГЖСШJЌГШЛЏЌЧШЛШВШЛЏЊSГТГШГГРЏЧSЏЛГГШСJJСJБЏЏЧГJЌJЌФГJЧJЛГSШУJЌГSГГШБJСГЏГSФЛГЛЖЛГФЏФИЖТЖСШЏJФЛJБШSЧШ
ФЛСJSШЖТSГЛЏГЛЏЊSГТГГЛЏГШЏШМГЛЏЛГГШГJЧЏВЖИЛШЛSШГВСJSЧЏЌSГЛЏВШИШУШКШSШSГСSГЛЏТИЏSJСГШСJЛЧЏSЌФJФСЏЛФГЃJЛЏЗЌЏЗSШГSHJЧЗ
ШЛГГШЛШФЏЏУJИЏЗГJЛГSЛЏЧЏФSШФЛЖЌЏSЛГЛЏВШJСШШJРИШФЛГФЏЏУJИЏЗГJЛЧШВСJБГЗJASJФЛГЛЏSШЌСШЛШГSФЛГЛЖЛГЌJСЏЌЖСШШЛЌЛJШСJЏJФИ
ЏЌSГЛЏЖТЏРSГУJЌГSГЌШФЛШSШЛSШБУJИЏЗГГSФЛГЛЖЛГSШНШГЖИЛЏЛГЛЏГЌШJЏФИЖАЖСШШЛФГJЧJЏJИJСГSШJЌФЛЖЌЏSЛГЛЏСJМЏИГJЛЏЏЧГJЌSШЧШВ
СJБЏJФЛJБШЛУJИЏЗРЧJБВШЏЗSГЏЧJЏГЛГГГФЛЧШАЖСШКШГШГJSШИГTSШЛШГШГSШГSФЛГЛЖМГJSШИSШJФSJСШЌСШЛШГSФЛГЛЖЛГРЏШСJЏJФЛJБШSШЛШЛ
ЧГШВШПЛJЏJСГФJГГСШИГЛЏЛSШФЛЖЌГГЛЏSШЖTSJГФЛЧШАЖСШТГШЛШГШЏИГГШЛГСSШЛШЌЏБSJФЛСШГСШЛШЛЧГШСФЖПSJФЛЧЏВЖИЛГЧШПЏФJЏЌЏSГJSЏТ
ЏSJРЏЌГSЖСШТГГНШГЛJЧФЏJBSШТГЛЏИЏSЧШВСJБГЏJЌЏ3SШГSHJЧЗШЛГГШЛШСJ3ШГЏЌJSГБШГНJЧ3ГЧШКЏSШЏЌSШГФГИЖТГЛЏИSJФГИSШВШЏЌSГМШSШ
ЃSHJЧЗШЛГТГГSШФJТЏSГSШФЛШСSГГШЌЧГJЌУJЌГSШЛГЏГНJЧ3ШИSJВШЏJTSЖСШШЛЌШТЏГJЧШЛЏJВШЏЌSГТГГЏШЛГШГJSШБФГИSШГSШБSШЏЧЏЌSШSШЖТ
SJГФЛЧШАЖСШТГШГJРЧШВJСSШГSФЛГЛЖМГБШСJ3ШГЏЌJSГБШJЌJРИШФЛГЛЏSШГSHJЧ3ШЛГГШЛШНШГЖИЛЏЛВШГSHJЧ3ШЛГТГГSШЖГГГГJ3ЏБЖЛЏЧФГJГS
АЏSЏЧФЛСJНЃSГГЌJЌГЏИJ3ФГГФЛЖЌГФГГЏЧJУЧШ3ГГJГНГSГГУГSЖЌГФЏФИЏЌSГЛЏГJ3ЏБЖЛЏЧФГГSШЖГГГJ3ЏБЖЛЏЧФГJГSАЏSЏЧФЛСJГSЛЏЧSЏЛГ3
ЧЏASШРЏВРЏЌSJФЛЏЧГ3ЏSШSШГSHJЧ3ШМЃФГГЛЏЊSJИJУГГГГJ3ЏБЖЛЏЧФГШЏЌЖГШМГБШФ3ЏЧJСГSШ3ШУГФЛЏЧФГГЏЌSJУJЌГПSГФЛЖЌГГФЏГSАЏSЏЧФ
ЛСJSШГSЛЏИГУЏSЛSГФГФЛЏ3ГГJ3ЏБЖЛЏЧФГГSШЖГГГJЌГЧШКЏГГЧГЏЛJУЧШНГБШФJНЛСЏЧФГJГSАЏSЏЧФЛСJГJ3ЏБЖЛЏЧФГГ3ЧЏАГГЏЛЏЊSJИJУГГГS
ЛЏИГУЏSЛSГГSНJЧ3ШМГJSГФГФЛЏ3ГФJНЛСЏЧФГJГSАЏSЏЧФЛСJФJЌЧАГSФГГРШВГЧШSJЏЧЏРШЧЖСШКЏРГJГSНJЧ3ШЛГГШЏГJГSНJЧ3ШЛГГШФГФЛЏ3СJ
ТГЏ

Важно е да се напомене дека овој текст е споен целиот т.е нема празни места помеѓу зборовите и со тоа дополнително се зголемува комплексноста за дешифрирање. За успешно пробивање и добивање на јасен текст се користеше напад со “фреквенција на букви” т.е дознаваме која буква колку често се користи и се прави споредба со најчесто користените букви во јазикот, што во овој случај е македонскиот јазик.

DECYPHER

За дешифрирање на пораката се користеше напад со фреквенција на букви во програмскиот јазик Java. Најнапред, начинот на кој се земаат буквите и истите се бројат како и процентуално се вадат е направено со две хешмапи. Во првата хешмапа чуваме character и integer (Map<Character, Integer> frequency = new HashMap<>()) и секоја буква ја читаме од баферот, посебно. Потоа проверуваме дали истата буква постои во мапата, доколку постои го зголемуваме бројачот (integer го претставува бројачот) на таа буква а во спротивно ја ставаме во мапата и го сетираме бројачот на 1. Втората користи character и float (Map<Character, Float> percent = new HashMap<>()). Овде ги сместуваме сите букви од првата мапа и соодветно за вредност ја поставуваме вредноста, процентуално, за тоа која буква колку пати се појавила. Излезот кој го добиваме е следниот (во прилог е дадена и табелата на најкористени букви во македонскиот јазик):

Буква	Фрекв. (%)	Буква во мак. јазик	Фрекв. (%)
Ѓ	12.114633	А	12.28
Ш	11.550152	О	10.98
Л	9.856709	И	9.93
J	9.422492	Е	9.52
S	8.55406	Т	7.27
Џ	7.468519	Н	7.00
Г	5.1671734	Р	5.52
Ф	4.9066434	С	4.98
Ч	4.515849	К	4.13
С	3.2566218	В	3.68
Ќ	3.1697788	Д	3.56
Ж	3.1263568	П	3.19
З	2.8224056	М	2.94
Ц	2.2145028	Л	2.59
И	2.1276596	У	2.08
Б	1.6066002	J	1.61
Н	1.6066002	З	1.60

В	1.4329137	Г	1.31
Т	1.2158055	Б	1.23
У	0.9552757	Ч	1.03
Р	0.8250109	Ц	0.89
А	0.7815892	Ш	0.72
М	0.43421626	Ж	0.57
Њ	0.34737298	Ф	0.43
К	0.30395138	Њ	0.33
П	0.21710813	Ќ	0.33
		Х	0.24
		Ѓ	0.05
		S	0.01
		Љ	0.00
		Џ	0.00

Најпрвин започнав со соодветна замена (Ѓ-А, Ш-О итн.) но добивав текстови што не ме асоцираа на ништо и со расфрлани македонски зборови за кои немав идеја како да ги спојам. Текстовите што ги добивав беа од облик на:

ЗОРПУИНИЕИГОАТЗЕКМОИА**БРАТ**ОПРААРЕМЛЈПИНКСРЕАТЖНТНКСИВЕЗАТРАВЕСР
ЕЛЈННЗЕКМАКОТВКГЕСТЕВОТО**ГОРЕТЕ**ИГОЕСТЕВОЌНТОЗОРПУИНИГОАТЗЕКМОИА
БРАТОПРААРЕМЛЈПИНКСРЕАТЖНТНКСИВЕВЕСЕСИОВТОПТАВНКГАИНИЕИСВРАКА
УАМНИЕДАЈСРЕЛЈНЕШЈОВНТВЕСУПЖШНТВНСТАРТОКМГОРЕТЕИСИОЛАТОСАУОТО
СНДМАЈОТПОКАДВНАУЈОДААНДАТОНСНИИОЦЕДАТОЗОРПУИНИЕИГОАТЗЕКМОИАБ
РАТОПРААРЕМЛЈПИНКСРЕАТЖНТНКСИВЕЗАТРАНКНГПУИОИТОГДКПЖПВОЌНИЕТО
ДВОИОТОЈЦЕУНМААТСИАИПИАЕДЕШУОСИОТОАТЗЕКМОИАРОИОАРЕМЛЈПИНКСРО
ИОИНЊТАРОВЕМОРНДЕТАЈОАТСИАИПИЕИГОАТЗЕКМОИАРОААЛКАЛКАКЕДТЕМОИ
НМОИАБРАЕИЗОРПУИНИААТСИАИПИЕИГОРЕМЛЈПИНКСРОИНЊТАРОААТЗЕКМОИА
РОАРИАЛКАЗОРПУИНИЕИГОНУНРИКЕИНЊТАРОААТЗЕКМОФАСРАИНЊТЕУЕЦААВЕ

Потоа одев со друга варијанта, повеќе комбинации на замена на првите 4 букви меѓусебно (првата од најчестите во текстот со третата најчеста од македонскиот јазик итн.) но добивав слични текстови. Едно нешто кое приметив беше тоа што дел од текстот се повторува на повеќе места.

Втор пристап кој што го имав беше со користење на биграми (листата на биграми се печати во Java кодот што го имам доставено и е многу голема, затоа не е опфатена во документот) но и тоа беше безуспешно.

Откако добив хинт дека текстот се работи за ФИНКИ, пробав други комбинации. Со самото тоа што претходно заклучив дека дел од текстот се повторува, прво што ми падна на памет беше дека тоа може да е зборот “Факултет”.

ЗОРПУИНИ→ ФАРПУЕНЕ

Во случајот Н → З (Н се заменуваше со З) па во кодот ги сменив местата на Н и З, Ш → О, се направи замена т.ш Ш → А, Ј →О, Л →Е. Од овде новодобиенот збор многу ми наликуваше на ФАКУЛТЕТОТ (водејќи се според позицијата на Е). Па така Н→Е, а Е→Т. Соодветно на ова ги сменив и Р→К, П→У и претхдното У→Л. Наредно што ми дојде на памет беше дека после Факултетот ќе следи ЗА ИНФОРМАТИЧКИ… Ја пробав и оваа комбинација, направив уште некои измени и дојдов до следниот текст:

ФАКУЛТЕТОТ ГА ИНФОРМАТИБКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО
ФИНКИ ВО СКОПЈЕ Е ФОРМИРАН ВРГ ОСНОВА НА ГАКОНОТГА ОСНОВА
ЌЕНАФАКУЛТЕТГАИНФОРМАТИБКИНАУКИИКОМПЈУТЕРСКОИНЖЕНЕРСТВОВОСОСТ
АВПАУПИВЕРГИТЕТОТСВКИРИЛИМЕТОДИЈСКОПЈЕОШЈАВЕПВОСЛУЖШЕПВЕСПИКП
ЛРМГАКОНОТСТАПИНАСИЛАНАСЕДМИЈАНУАРИДВЕИЛЈАДИИЕДИНАЕСЕТТАЦОДИН
ЛФАКУЛТЕТОТГАИНФОРМАТИБКИНАУКИИКОМПЈУТЕРСКОИНЖЕНЕРСТВОФИНКИЕР
ЕГУЛТАТНАГДРУЖУВАЌЕТОНАДВАТАНАЈЦОЛЕМИИИНСТИТУПИОДОШЛАСТАНАИНФО
РМАТИКАТАЙКОМПЈУТЕРСКАТАТЕЊНИКАВОМАКЕДОНИЈАИНСТИТУТОТГАИНФОРМ
АТИКАИИПРИПРИРОДНОМАТЕМАТИБКИОТФАКУЛТЕТИИНСТИТУТОТГАКОМПЈУТЕРС
КАТЕЊНИКАИИНФОРМАТИКАИКТИПРИФАКУЛТЕТОТГАЕЛЕКТРОТЕЊНИКАИИНФОР
МАЗИСКИТЕЊНОЛОЦИИВОДАДЕНАТАФОРМАДВАТАИНСТИТУТИРАПОТАТУХТЕОДО
СУМДЕСЕТТИТЕЦОДИНИНАМИНАТИОТВЕКИИПОБНУВАДАРАШОТИОДДАЛЕБНАТАО
СУМДЕСЕТИПЕТТАЦОДИНАКАКОРАМНОПРАВНАСОСТАВНАЗЕЛИНАНАПОВТОРНОО

Во случајот веќе станува јасно за што се работи. Со разделување на зборовите се доловува смислата на текстот и уште некои дополнителни измени се прават за да се дојде до оригиналниот текст (во случајот првин ВРГ→ВРЗ т.е Г→З, важно е да се напомене бидејќи доколку првин го смениме Ц → Г па Г→З, тоа ќе ја смени и ГОДИНА во ЗОДИНА. Па ЦОДИНА → ГОДИНА т.е Ц→Г, и измени од сличен облик).

Пермутацијата користена во овој пример е следната:
Ѓ=И, S=Н, Ј=О, Њ=Х, Ќ=Д, Џ=Е, А=Ж, Б=Ј, В=З, Г=К, Ж=У, З=М, И=Л, К=Њ, Л=Т, М=Ц, Н=Ф, П=Ш, Р=Б, С=В, Т=Ч, У=Г, Ф=С, Ц=П, Ч=Р, Ш=А

Добиениот текст откако ќе се заменат соодветните букви изгледа вака:

ФАКУЛТЕТОТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО ФИНКИ ВО СКОПЈЕ Е ФОРМИРАН ВРЗ ОСНОВА НА ЗАКОНОТ ЗА ОСНОВАЊЕ НА ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО ВО СОСТАВ НА УНИВЕРЗИТЕТОТ СВ КИРИЛ И МЕТОДИЈ СКОПЈЕ ОБЈАВЕН ВО СЛУЖБЕН ВЕСНИК НА РМ ЗАКОНОТ СТАПИ НА СИЛА НА СЕДМИ ЈАНУАРИ ДВЕ ИЛЈАДИ И ЕДИНАЕСЕТТА ГОДИНА ФАКУЛТЕТОТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО ФИНКИ Е РЕЗУЛТАТ НА ЗДРУЖУВАЊЕТО НА ДВАТА НАЈГОЛЕМИ ИНСТИТУТИ ОД ОБЛАСТА НА ИНФОРМАТИКАТА И КОМПЈУТЕРСКАТА ТЕХНИКА ВО МАКЕДОНИЈА ИНСТИТУТОТ ЗА ИНФОРМАТИКА ИИ ПРИ ПРИРОДНО МАТЕМАТИЧКИОТ ФАКУЛТЕТ И ИНСТИТУТОТ ЗА КОМПЈУТЕРСКА ТЕХНИКА И ИНФОРМАТИКА ИКТИ ПРИ ФАКУЛТЕТОТ ЗА ЕЛЕКТРОТЕХНИКА И ИНФОРМАЦИСКИ ТЕХНОЛОГИИ ВО ДАДЕНАТА ФОРМА ДВАТА ИНСТИТУТИ РАБОТАТ УШТЕ ОД ОСУМДЕСЕТТИТЕ ГОДИНИ НА МИНАТИОТ ВЕК ИИ ПОЧНУВА ДА РАБОТИ ОД ДАЛЕЧНАТА ОСУМДЕСЕТ И ПЕТТА ГОДИНА КАКО РАМНОПРАВНА СОСТАВНА ЦЕЛИНА НА ПОВТОРНО ОБЕДИНЕТИОТ ПМФ ПОД ИМЕТО ИНСТИТУТ ЗА ИНФОРМАТИКА ИКТИ ПОТЕКНУВА ОД КАТЕДРАТА ЗА ТЕХНИЧКА КИБЕРНЕТИКА ВО ОВОЈ ПЕРИОД ОД СКОРО ТИНА ГОДИНИ КАЈ ОВИЕ ИНСТИТУТИ СЕ СЛУЧУВА ПОСТОЈАН РАСТ ВО НАУЧНИТЕ И ТЕХНИЧКИТЕ КАПАЦИТЕТИ КАКО РЕЗУЛТАТ НА ИЗВОНРЕДНИТЕ ЗАЛАГАЊА НА НИВНИТЕ ЧЛЕНОВИ А ВО ТРЕНД СО СВЕТСКИОТ ПОДЕМ НА ИНФОРМАТИКАТА СПО ГОЛЕМИОТ ИНТЕРЕС НА СТУДЕНТИТЕ ЗА ОВАА ОБЛАСТ И СПО ГОЛЕМИОТ РАЗВОЈ И МОЖНОСТИТЕ НА ДВАТА ИНСТИТУТИ ДОВЕДУВААТ ДО ТОА ВО ПОСЛЕДНИТЕ УЧЕБНИ ГОДИНИ ДА СТАНАТ НАЈГОЛЕМИ ИНСТИТУТИ НА ФАКУЛТЕТИТЕ И ДА ОПСЛУЖУВААТ СКОРО ПОЛОВИНА ОД СТУДЕНТИТЕ ВО ЦЕЛИОТ ПЕРИОД НА РАЗВОЈ ПОСТОЈАТ ГОЛЕМ БРОЈ ЗАЕМНИ ПРОЕКТИ И ИСТРАЖУВАЊА КАКО НА ЛИЧНА ТАКА И НА ИНСТИТУЦИОНАЛНА ОСНОВА ДВАТА ИНСТИТУТИ БЕА ВО ПОСТОЈАНАТА ТРКА ЗА ШТО ПОВИСОК КВАЛИТЕТ НА СТУДИИТЕ НАУЧНО ИСТРАЖУВАЧКАТА И АПЛИКАТИВНАТА ДЕЈНОСТ ВАКВАТА ТРКА ВСУШНОСТ РЕЗУЛТИРАШЕ СО ЕДЕН КОНЕЧЕН ОБЕДИНУВАЧКИ ФАКТОР СПО ЗНАЧИТЕЛЕН РАЗВОЈ И ПОДЕМНА ИНФОРМАТИКАТА ВО МАКЕДОНИЈА И ФОРМИРАЊЕ НА ЕДНА ИСКЛУЧИТЕЛНО СИЛНА ЗАЕДНИЦА НА ИНФОРМАТИЧКИ НАСОЧЕНИ НАСТАВНИ КАДРИ ОД ГОДИНА ТИЕ И ФОРМАЛНО ЗАПОЧНУВААТ ДА

ЧЕКОРАТ ПО ЗАЕДНИЧКИ ПАТ КАКО НАЈСИЛНА И НАЈНАПРЕДНА НАУЧНО ИСТРАЖУВАЧКА И ОБРАЗОВНА ИНСТИТУЦИЈА ВО МАКЕДОНИЈА ОД ОБЛАСТИТЕ НА ИНФОРМАТИКАТА ФАКУЛТЕТ ЗА ИНФОРМАТИЧКИ НАУКИ И КОМПЈУТЕРСКО ИНЖЕНЕРСТВО ФИНКИ ДОДИПЛОМСКИ СТУДИСКИ ПРОГРАМИ КОИ ФИНКИ ГИ НУДИ СЕ СЛЕДНИТЕ КОМПЈУТЕРСКИ НАУКИ КОМПЈУТЕРСКО ИНЖЕНЕРСТВО ИНТЕРНЕТ И МРЕЖНА БЕЗБЕДНОСТ ПРИМЕНА НА ИНФОРМАЦИСКИ ТЕХНОЛОГИИ И КОМПЈУТЕРСКА ЕДУКАЦИЈ А СМЕРОВ И НА МАГИСТЕРСК И ЕДНОГОДИШНИ СТУДИИ СЕ ИНЖЕНЕРСТВО НА ИНТЕЛИГЕНТНИ СИСТЕМИ КОМПЈУТЕРСКИ НАУКИ КОДИРАЊЕ И КРИПТОГРАФИЈА СОФТВЕРСКО ИНЖЕНЕРСТ ВО КОМПЈУТЕРСКИ МРЕЖИ И Е-ТЕХНОЛОГИИ ИНТЕЛИГЕНТНИ ИНФОРМАЦИОНИ СИСТЕМ И СОФТВЕРСКО ИНЖЕНЕРСТВО СОДРЖИНСКИ БАЗИРАНО ПРЕБАРУВАЊЕ БИОИНФОРМАТИКА ЕКОИНФОРМАТИКА СИСТЕМ ВО ЧИП