Лекція №2 (НЕ 1.2, 2 год.). Класичні техніки шифрування.

План лекції:

1. Шифри перестановок.
2. Шифри підстановок.

Зміст лекції:

Розглянемо деякі класичні техніки шифрування.

1. Шифри перестановок.

1. Шифр частоколу.

Одним з найпростіших шифрів перестановки є т.зв. шифр частоколу. Він дуже схожий на матричний шифр. Для прикладу зашифруємо цим шифром з висотою частоколу 2 слово «*зашифрування*». Для цього запишемо його таким чином:

а и р в н я

з ш ф у а н

Тепер зчитуємо спочатку верхній рядок: «*аирвня*», а потім – нижній: «*зшфуан*». Отже зашифроване повідомлення: «*аирвнязшфуан*».

Для частоколу висотою 3 отримаємо такий зашифрований текст:

ш р а я

а ф в н - «*шраяафвнзиун*»

з и у н

2. Матричний шифр.

Відкритий текст записують послідовно рядок за рядком у матрицю. Літери криптограми виписують з цієї ж матриці по стовпчиках. Для прикладу зашифруємо текст «*припиніть скуповувати акції*» на матриці 5×5.

п	р	и	п	и
н	і	т	ь	с
к	у	п	о	в
у	в	а	т	и
а	к	ц	і	ї

Зчитуючи літери по стовпчиках, отримаємо шифрограму: «*пнкуа ріувк итпац пьоті исвиї*». Зрозуміло, що криптостійкість такого шифру зовсім незначна, однак її можна легко підсилити. Для цього використовують ключові слова. Зашифруємо цю ж фразу на ключах «*біржа*» і «*товар*». Ключі записуємо згори та зліва від матриці тексту, після чого переставляємо рядки та стовпчики згідно з позицією кожної літери ключів у абетці. Отже матриця з відкритим текстом перетворюється наступним чином.

	б	**і**	**р**	**ж**	**а**
т	п	р	и	п	и
о	н	і	т	ь	с
в	к	у	п	о	в
а	у	в	а	т	и
р	а	к	ц	і	ї

→

	а	**б**	**ж**	**і**	**р**
а	и	у	т	в	а
в	в	к	о	у	п
о	с	н	ь	і	т
р	ї	а	і	к	ц
т	и	п	п	р	и

Отримаємо шифротекст: «*ивсїи украп тоьіп вуікр аптци*».

Розшифрувати шифрограму можна, записавши слова у матрицю по стовпчиках згідно з порядком слідування літер ключів, а потім, переставивши стовпчики та рядки так, щоби ключі утворили зв‘язні слова, зчитуємо розшифрований текст по рядках.

Дешифрувати повідомлення без знання ключів можна, якщо проаналізувати записаний по стовпчиках шифротекст на частоту появлення пар літер, тобто на тому, що деякі пари літер ніколи не зустрічаються або зустрічаються в українській мові дуже рідко.

3. Шифр Першої світової війни (ADFGVX-шифр).

Модифікацією матричного шифру можна вважати ADFGVX-шифр, який використовували під час Першої світової війни [Мельник]. Це комбінація підстановки та перестановки за ключовим словом. Припустимо, для прикладу, що необхідно зашифрувати текст «*don't put it off till tomorrow*" (не відкладайте це до завтра). Використаємо таблицю 6×6, в яку впишемо усі латинські літери та цифри від 0 до 9.

	A	**D**	**F**	**G**	**V**	**X**
A	C	O	8	X	F	4
D	M	K	3	A	Z	9
F	N	W	L	0	J	D
G	5	S	I	Y	H	U
V	P	1	V	B	6	R
X	E	Q	7	T	2	G

Для зашифрування фрази знаходимо почергово її літери у таблиці та вибираємо літери, які стоять у заголовках рядка та стовпчика. Таким чином *d* перетворюється у *FX*, *o* – *AD*, *n* – *FA* і т.д. В результаті отримуємо таку шифрограму:

FXADFAXGVAGXXGGFXGADAVAVXGGFFFFFXGADDAADVXVXADFD.

Застосуємо тепер матричний шифр на ключі *GARDEN*.

G	**A**	**R**	**D**	**E**	**N**
4	1	6	2	3	5
F	X	A	D	F	A
X	G	V	A	G	X
X	G	G	F	X	G
A	D	A	V	A	V
X	G	G	F	F	F
F	F	X	G	A	D
D	A	A	D	V	X
V	X	A	D	F	D

Записавши літери шифрограми по стовпчиках в порядку зростання цифр, отримаємо:

XGGDGFAXDAFVFGDDFGXAFAVFFXXAXFDVAXGVFDXDAVGAGXAA.

2. Шифри підстановок.

1. Шифр Цезаря.

Цей шифр реалізує таке перетворення відкритого тексту: кожна літера замінюється третьою після неї літерою того ж алфавіту, який вважається написаним по колу, тобто після „я" йде „а". Відмітимо, що Юлій Цезарь замінював кожну літеру третьою за нею літерою, але можна міняти й будь-якою іншою. Головне, щоби адресат цього повідомлення знав величину і напрямок цього зсуву.

Криптостійкість шифру Цезаря можна підсилити, побудувавши таблицю заміни за ключовим словом, або використавши т.зв. афінну систему Цезаря, коли величина зсуву різна для кожної літери повідомлення. Цим шифрам присвячена робота №3 лабораторного практикуму з криптографії та розглядається на практичних заняттях.

2. Шифр пар.

Шифр пар використовує ключову фразу, яка легко запам‘ятовується та містить, як правило, близько половини літер абетки. Для того, щоби зашифрувати повідомлення, вчиняють так. Ключову фразу записують в один рядок, причому літери, які подвоюються, вилучаються. У випадку української мови, коли в абетці 32 літери, 16 літер ключової фрази записують у верхньому рядку, а решту 16 літер – у нижньому рядку в порядку їх слідування в абетці. Таким чином, ми створили таблицю заміни, яку тепер можна використати для зашифрування повідомлення [Мельник].

Для прикладу створимо таблицю заміни на ключовій фразі «Реве та стогне Дніпр широкий».

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
р	е	в	т	а	с	о	г	н	д	і	п	ш	и	к	й
б	ґ	є	ж	з	л	м	у	ф	х	ц	ч	щ	ь	ю	я

Зашифруємо за допомогою цієї таблиці заміни повідомлення: «*Чекайте літак завтра опівночі*». Шифротекст буде мати вигляд: «*Пгюзяжт сцжзю азєжбз мчцєфмпц*». Для розшифрування криптограми використовують таку саму таблицю, замінюючи за нею літери шифротексту.

3. Квадрат Полібія.

і	ж	ю	о	в	а
з	н	и	ш	ь	я
б	д	л	ф	є	ч
м	е	щ	й	п	г
к	у	т	х	ї	с
ц	р	.	,	-	;

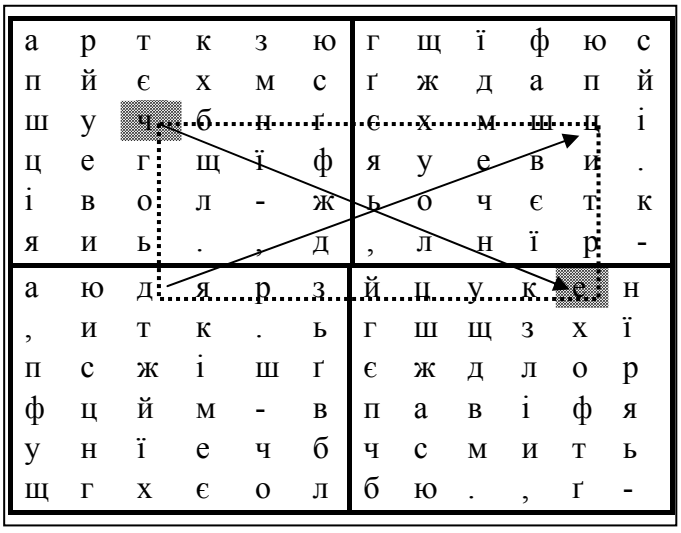
Ще одним прикладом шифрів підстановки є квадрат, що отримав ім‘я грецького письменника Полібія, - полібіанський квадрат. Вперше він був розроблений для грецької абетки. Для української мови квадрат Полібія може мати такий вигляд:

Для зашифрування повідомлення квадрат використовується наступним чином. Кожна літера відкритого тексту замінюється на літеру, що знаходиться точно під нею. Якщо літера стоїть в останньому рядочку – вона замінюється такою, що стоїть у першому рядочку точно над нею. Отже повідомлення «Зустріч перенесено на завтра» перетворюється у «*Бр;.жзг їужуду;удш дя бяь.жя*».

4. Шифр Play-fair.

Шифр Play-fair було розроблено для англійської абетки. Двадцять п‘ять літер (*i* та *j* ототожнювалися) у випадковому порядку розміщувалися у квадраті розміром 5×5. Для зашифрування використовують від одного до чотирьох квадратів. Якщо використовується один квадрат, він називається «магічним». З чотирма квадратами криптостійкість шифру зростає, оскільки невідомим залишається розміщення літер у чотирьох, а не в одному квадраті. Крім того, не буває критичних ситуацій, коли обидві літери знаходяться в одному рядку або стовпчику.

Реалізуємо варіант цього шифру для української абетки. Використаємо для цього чотири квадрати 6×6, заповнивши їх у випадковому порядку літерами та знаками пунктуації.



Для прикладу зашифруємо повідомлення «*Чекайте літак завтра опівночі*». Розіб‘ємо його на пари літер: «*Че ка йт ел іт ак за вт ра оп ів но чі*». Щоби зашифрувати пару «*Че*», шукаємо «*Ч*» в першому квадраті, «*е*» - в четвертому. Вони позначені у таблиці штриховкою. Ці літери утворюють прямокутник і знаходяться на його діагоналі (вона позначена стрілкою). На іншій діагоналі знаходяться літери «*Д*» та «*ц*». Отже пара «*Че*» замінюється на «*Дц*». Подібним чином «*ка*» переходить в «*іщ*», «*йт*» - в «*нп*» і так далі. В результаті отримаємо криптограму: «*Дціщнпсвутаф-щнтцщйьфчшцйш*».

5. Шифр Віженера.

Шифр Віженера, як це вже згадувалося, відноситься до багатоалфавітної заміни. Використовується відкрите повідомлення та ключове слово або фраза. Якщо довжина ключового слова не збігається з довжиною повідомлення, слово повторюють кілька разів. Зашифровують повідомлення за допомогою так званої таблиці Віженера, яку легко скласти самостійно.

	а	**б**	**в**	**г**	**д**	**е**	**є**	**ж**	**з**	**и**	**і**	**ї**	**й**	**к**	**л**	**м**	**н**	**о**	**п**	**р**	**с**	**т**	**у**	**ф**	**х**	**ц**	**ч**	**ш**	**щ**	**ь**	**ю**	**я**
а	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я
б	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а
в	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б
г	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в
д	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г
е	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д
є	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е
ж	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є
з	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж
и	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з
і	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и
ї	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і
й	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї
к	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й
л	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к
м	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л
н	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м
о	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н
п	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о
р	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п
с	с	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р
т	т	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с
у	у	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т
ф	ф	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у
х	х	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф
ц	ц	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х
ч	ч	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц
ш	ш	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч
щ	щ	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш
ь	ь	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ
ю	ю	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь
я	я	а	б	в	г	д	е	є	ж	з	и	і	ї	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ь	ю

Припустимо, що нам треба зашифрувати повідомлення: «*Переходьте до виконання плану номер два*» на ключі «*резидент*».

п	е	р	е	х	о	д	ь	т	е	д	о	в	и	к	о	н	а	н	н	я	п	л	а	н	у	н	о	м	е	р	д	в	а
р	е	з	и	д	е	н	т	р	е	з	и	д	е	н	т	р	е	з	и	д	е	н	т	р	е	з	и	д	е	н	т	р	е
е	ї	ш	л	щ	у	к	п	з	і	й	ч	є	л	ь	є	г	е	х	ц	г	ф	ю	т	г	ш	х	ч	р	і	г	ц	т	е

Як можна зрозуміти з наведеної таблиці, шифрування виконується таким чином. Літеру повідомлення, наприклад «п», шукають у лівому стовпчику таблиці Віженера. Літеру ключового слова, наприклад «*р*» шукають у верхньому рядку. На перетині рядка з літерою «*п*» та стовпчика з літерою «*р*» знаходиться літера «*е*». Отже після зашифрування отримаємо такий шифротекст: «*еішлдукпзійчєльєгехцгфютгшхчрігцте*».

Процес розшифрування виконується наступним чином. У стовпчику зліва шукаємо літеру ключа, наприклад «*р*». Далі, шукаємо у рядочку з цією «*р*» літеру шифротексту «*е*» і дивимося, в якому стовпчику вона стоїть. Заголовок цього стовпчика, у нашому випадку «*п*», і буде розшифрованим текстом.

Як бачимо, навіть однаковим літерам відкритого тексту можуть відповідати різна літери шифротексту, що значно ускладнює дешифрування. Однак це не означає, що цей шифр не можна дешифрувати за допомогою аналізу частот появи різних літер та їх блоків у зашифрованому тексті.

Класичні техніки шифрування сьогодні втратили свою цінність як самостійні шифри. Криптостійкість їх дуже незначна, до того ж існує багато програмних засобів, які легко їх розкривають. Однак вони не втратили своєї актуальності, оскільки, по-перше, з них варто починати вивчення криптографії, а по-друге, вони можуть бути складовими частинами серйозніших сучасних систем шифрування, які розглядаються далі у цій книзі.