Лабораторна робота № 1.

Класичні техніки шифрування.

Шифри перестановок.

Шифр Першої світової війни (ADFGVX-шифр).

Модифікацією матричного шифру можна вважати ADFGVX-шифр, який використовували під час Першої світової війни. Це комбінація підстановки та перестановки за ключовим словом. Припустимо, для прикладу, що необхідно зашифрувати текст *«monday is the key change day"* (понеділок – день зміни ключа). Використаємо таблицю 6х6 (табл.1), в яку впишемо всі латинські літери та цифри від 0 до 9.

Таблиця 1

Таблиця для ADFGVX-шифру

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

Для зашифрування фрази знаходимо почергово її літери в таблиці та вибираємо літери, які стоять у заголовках рядка та стовпчика. Отже, *m* перетворюється в *AD, o* - в *DA, n* – в *AF* і т.д. У результаті отримуємо таку шифрограму:

ADDAAFXFGVGFFFDGGAVGAXDDAXGFAAVGGVAFXXAXXFGVGF.

Аналогічно можна створити схожі шифри для української і російської мов.

Шифри підстановок.

Шифр Play-fair

Шифр Play-fair розроблено для англійської абетки. Двадцять п'ять літер *(i*

та *j* ототожнювалися) у випадковому порядку розміщувалися у квадраті розміром 5х5. Для зашифрування використовують від одного до чотирьох квадратів. Якщо використовується один квадрат, він називається «магічним». Із 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 6х6, 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»* у першому квадраті, «є» – в четвертому. Вони позначені в таблиці штриховкою (рис. 1).

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

Рис. 1. – Таблиці шифру Play-fair для української абетки

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 *«мщ»*, *«йт»* – у *«нп»* і так далі.

У результаті отримаємо криптограму: *«Дцвщнпсвутаф-щнтцщйьфчшцйш»*.

Завдання роботи.

1. Оберіть народне прислів’я українською мовою.
2. Зашифруйте його за допомогою ADFGVX-шифру для української абетки.
3. Зашифруйте його за допомогою шифру Play-fair, що складається з чотирьох квадратів 6x6.
4. Підгрупа розбивається на пари за бажанням. Члени пари обмінюються між собою ключами та зашифрованими повідомленнями, здійснюють дешифрування цих повідомлень.