Запорізький національный університет

Основи безпеки інформаційних систем

І.В.Козін

Задачі лекції

1. Шифрування даних
2. Резервне копіювання

Шифрування даних

Шифрування являє собою приховування інформації від неавторизованих осіб з наданням в цей же час авторизованим користувачам доступу до неї. Користувачі називаються авторизованими, якщо у них є відповідний ключ для дешифрування інформації.

Метою будь-якої системи шифрування є максимальне ускладнення отримання доступу до інформації неавторизованими особами, навіть якщо у них є зашифрований текст і відомий алгоритм, використаний для шифрування. Поки неавторизований користувач не володіє ключем, секретність і цілісність інформації не порушується.

Шифрування даних

За допомогою шифрування забезпечуються три стану безпеки інформації:

Конфіденційність. Шифрування використовується для приховування інформації від неавторизованих користувачів при передачі або при зберіганні.

Цілісність. Шифрування використовується для запобігання зміни інформації при передачі або зберіганні.

Ідентифікованість. Шифрування використовується для аутентифікації джерела інформації та запобігання відмови відправника інформації від того факту, що дані були відправлені саме їм.

Шифрування даних

Звичайний текст - інформація в початковому вигляді. Також називається відкритим текстом.

Шифрований текст - інформація, піддана дії алгоритму шифрування.

Алгоритм - метод, який використовується для перетворення відкритого тексту в шифрований текст.

Ключ - Вхідні дані, за допомогою яких за допомогою алгоритму відбувається перетворення відкритого тексту в шифрований або назад.

Шифрування - Процес перетворення відкритого тексту в шифр.

Дешифрування - Процес перетворення шифру у відкритий текст.

Шифрування даних

Звичайний текст - інформація в початковому вигляді. Також називається відкритим текстом.

Шифрований текст - інформація, піддана дії алгоритму шифрування.

Алгоритм - метод, який використовується для перетворення відкритого тексту в шифрований текст.

Ключ - Вхідні дані, за допомогою яких за допомогою алгоритму відбувається перетворення відкритого тексту в шифрований або назад.

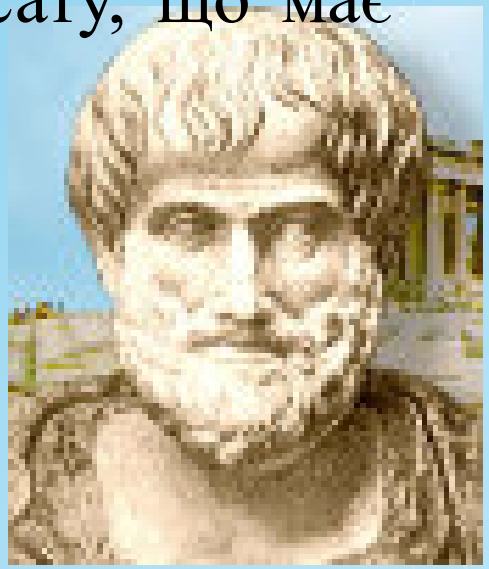
Шифрування - Процес перетворення відкритого тексту в шифр.

Дешифрування - Процес перетворення шифру у відкритий текст.

Шифрування даних

Хитромудрий спосіб шифрування був винайдений в стародавній Спарті за часів Лікурга (V століття до н.е.). Для зашифровування тексту використовувалася Сціталла - жезл циліндричної форми, на який намотувалася стрічка з пергаменту. Уздовж осі циліндра через підрядник записувався текст, стрічка змотувалася з жезла і передавалася адресату, що має Сціталлу такого ж діаметру. Цей спосіб здійснював перестановку букв повідомлення. Ключем шифру служив діаметр Сціталли.

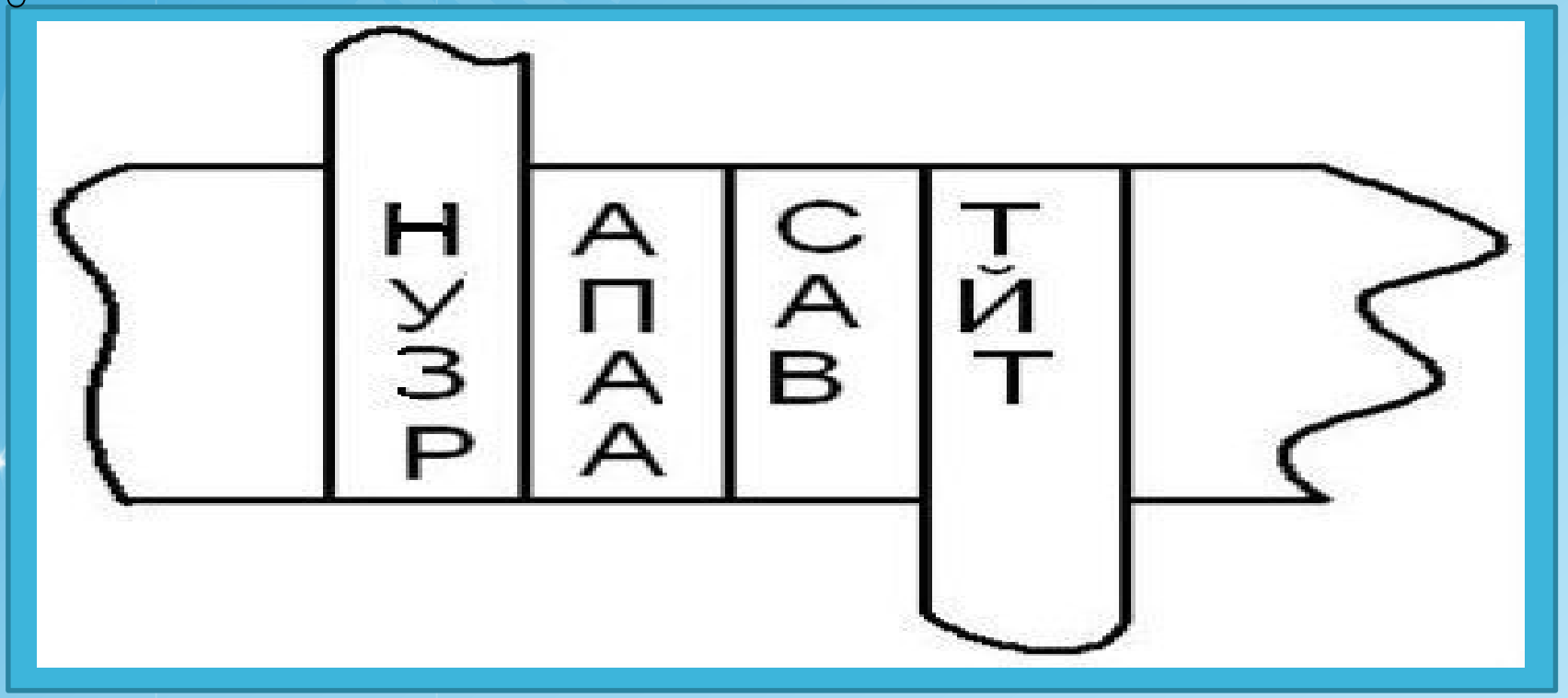
АРИСТОТЕЛЬ придумав метод розкриття такого шифру.



Шифрування даних

Розшифруйте повідомлення, передане спартанцю в V століття до н. е.

НУЗРАПААСАВТЙТ



Шифрування даних

Греческий писатель ПОЛИБИЙ использовал систему сигнализации, которая применялась как метод шифрования. С его помощью можно было передавать абсолютно любую информацию. Он записывал буквы алфавита в квадратную таблицу и заменял их координатами.

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

Устойчивость этого шифра была велика. Основная причина - возможность постоянно менять в квадрате последовательность букв.

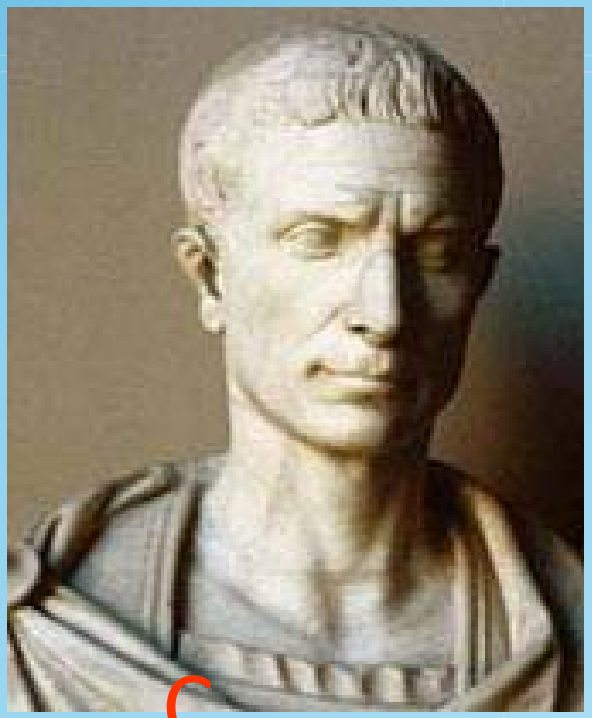
Шифрування даних

Розшифруйте повідомлення,
6364433216626436111234421142546441645224443634326564116442556 6

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

Я умею работать с шифром! А ты?

Шифрування даних



Особливу роль в збереженні таємниці зіграв спосіб шифрування, запропонований Юлієм Цезарем і описаний ним в «Записках про галльську війну» (1 століття до н.е.) Ключем в шифрі Цезаря є величина зсуву на 3.

Зашифруємо слово КОД (рос.)

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

Отримуємо слово НСЖ

Шифрування даних

Розшифруйте повідомлення

ТУЛЫИО, ЦЕЛЖЗО,ТСДЗЖЛО!

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

Алгоритм шифрування: читати четверту букву замість першої.

ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ!

Шифрування даних

Існує кілька модифікацій шифру Цезаря. Один з них алгоритм шифру Гронсфельда (створений в 1734 році бельгійцем Хосе де Бронкхором, графом де Гронсфельда, військовим і дипломатом). Шифрування полягає в тому, що величина зсуву не є постійною, а задається ключем (гамою).

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

При заданному ключі 317413327121 з шифротексту НСПУУСЁТЖХКА отримуємо:

Криптография

Шифрування даних

Для того, хто передає шифровку, важлива її стійкість до дешифрування. Ця характеристика шифру називається криптостійкостю. Підвищити криптостійкість дозволяють шифри багатоалфавітної або багатозначної заміни. У таких шифрах кожному символу відкритого алфавіту ставляться у відповідність не один, а кілька символів шифровки.

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П	Р
21	37	14	22	01	24	62	73	46	23	12	08	27	53	35	04
40	26	63	47	31	83	88	30	02	91	72	32	77	68	60	44
10	03	71	82	15	70	11	55	90	69	38	61	54	09	84	45

Шифрування даних

Наукові методи в криптографії вперше з'явилися в арабських країнах. Арабського походження і саме слово шифр (від арабського «цифра»). Араби першими стали замінювати літери цифрами з метою захисту вихідного тексту. Перша книга, спеціально присвячена опису деяких шифрів, з'явилася в 855г., Вона називалася «Книга про велике прагнення людини розгадати загадки древньої писемності».

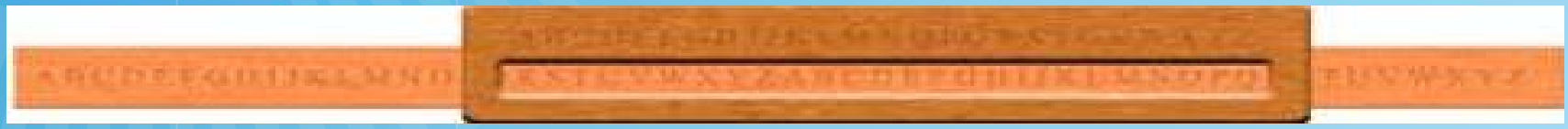
Шифрування даних

Італійський математик і філософ Джироламо Кардано написав книгу "Про тонкощі", в якій є частина, присвячена криптографії. Кардано дає "доказ" стійкості шифрів, засноване на підрахунку числа ключів, пропонує використовувати відкритий текст в якості ключа, і новий шифр, "Решітка Кардано".

Решітка являє собою лист з твердого матеріалу, в якому через неправильні інтервали зроблені прямокутні вирізи висотою для одного рядка і різної довжини. На лист накладали цю решітку і записували в вирізи секретне повідомлення. Решту місць заповнювалися довільним текстом.

Шифрування даних

В конце XIX века криптография начинает приобретать черты точной науки, а не только искусства, ее начинают изучать в военных академиях. В одной из них был разработан свой собственный военно-полевой шифр, получивший название "Линейка Сен-Сира".



В 80-х годах XIX века ОГЮСТ КЕРКГОФФС издал книгу "Военная криптография" объемом всего в 64 страницы, но они обессмертили его имя в истории криптографии. В ней сформулированы шесть конкретных требований к шифрам. Все эти требования актуальны и в наши дни.

Шифрування даних

Во второй половине XX века, вслед за развитием элементной базы вычислительной техники, появились электронные шифраторы. Сегодня они составляют подавляющую долю средств шифрования, удовлетворяя все возрастающим требованиям по надежности и скорости шифрования. В семидесятых годах был принят и опубликован первый стандарт шифрования данных (DES), "легализовавший" принцип Керкгоффса в криптографии; после работы американских математиков У. ДИФФИ и М. ХЕЛЛМАНА родилась "новая криптография"— криптография с открытым ключом.

Кодування даних

Капитан французской армии ШАРЛЬ БАРБЬЕ разработал в 1819 году систему кодирования ecriture noctrume – ночное письмо. В системе применялись выпуклые точки и тире, недостаток системы её сложность, так как кодировались не буквы, а звуки. ЛУИ БРАЙЛЬ усовершенствовал систему, разработал собственный шифр. Основы этой системы используются и сейчас.

Кодування даних

СЭМЮЕЛЬ МОРЗЕ разработал в 1838 году систему кодирования символов с помощью точки и тире.

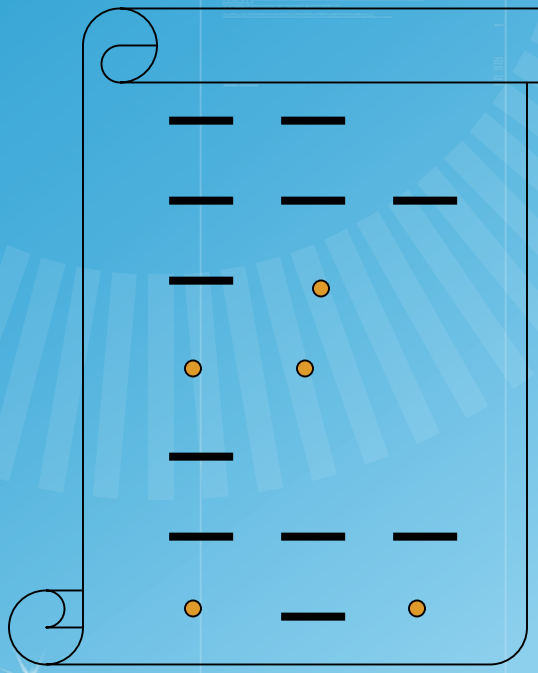
Он является изобретателем телеграфа (1837год) – устройства в котором использовалась эта система. Самое важное в этом изобретении – двоичный код,- использование для кодирования букв только двух символов.

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

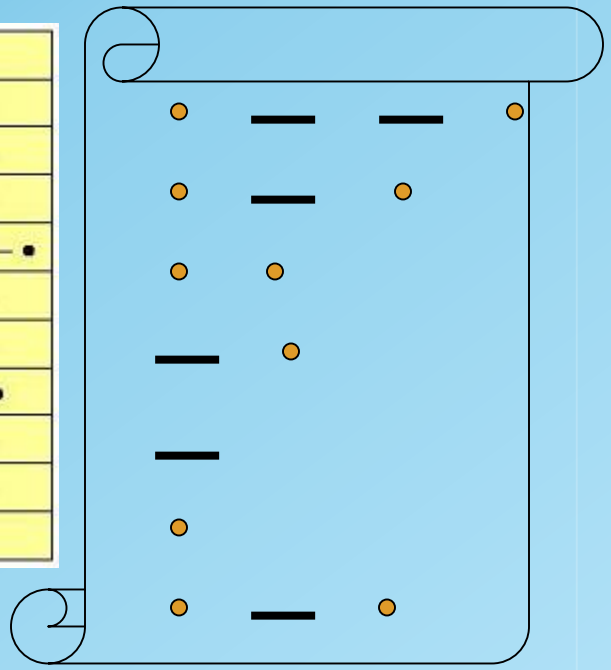
1 ·––––	2 ··–––	3 ···––	4 ····–
5 ·····	6 –····	7 ––···	8 –––··
9 ––––·	0 –––––		

Кодування даних

Розшифруйте повідомлення:



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



А що буде далі…

..ну що, нарешті ...

Пора прощатися.

До побачення!