Тема. Основи криптографічних методів захисту інформації

Студент групи СН-41

Стойко Володимир Ігорович

Обмін інформацією у відкритому вигляді

Відправник

Адресат

Повідомлення

Несанкціонований доступ

Зміст повідомлення

Обмін інформацією, що шифрується

Відправник

Повідомлення

Механізм шифрування

Зашифроване повідомлення

Адресат (із ключем шифру)

Несанкціонований доступ

Незрозуміла інформація, яку, отже, неможливо використати

Квадрат Полібія

	1	2	3	4	5	6
1	А	Б	В	Г	Ґ	Д
2	Е	Є	Ж	З	И	І
3	Ї	Й	К	Л	М	Н
4	О	П	Р	С	Т	У
5	Ф	Х	Ц	Ч	Ш	Щ
6	Ь	Ю	Я			

Метод №1

Буква тексту	з	а	х	и	с	т
Буква шифротекст	г	ь	п	ґ	л	м

Метод №2

Букви	з	а	х	и	с	т
X	2	1	5	2	4	4
Y	4	1	2	5	4	5

21 52 44 41 25 45

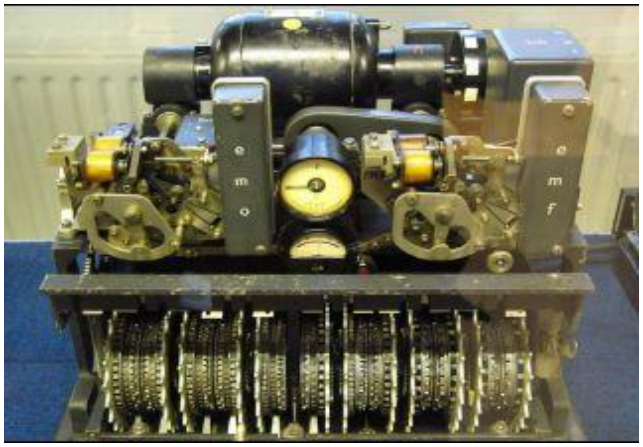
X	2	5	4	4	2	4
Y	1	2	4	1	5	5
Букви	е	х	с	о	и	т

Текст	з	а	х	и	с	т
Шифр	е	х	с	о	и	т

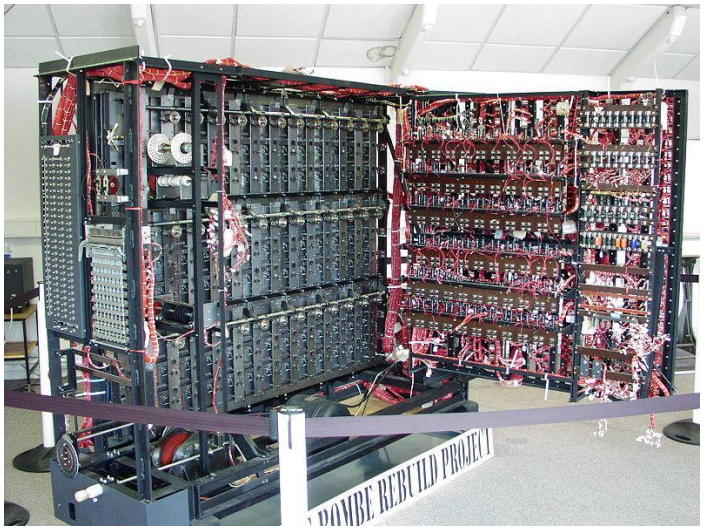
Криптомашини у другій світовій війні

Enigma

Lorenz



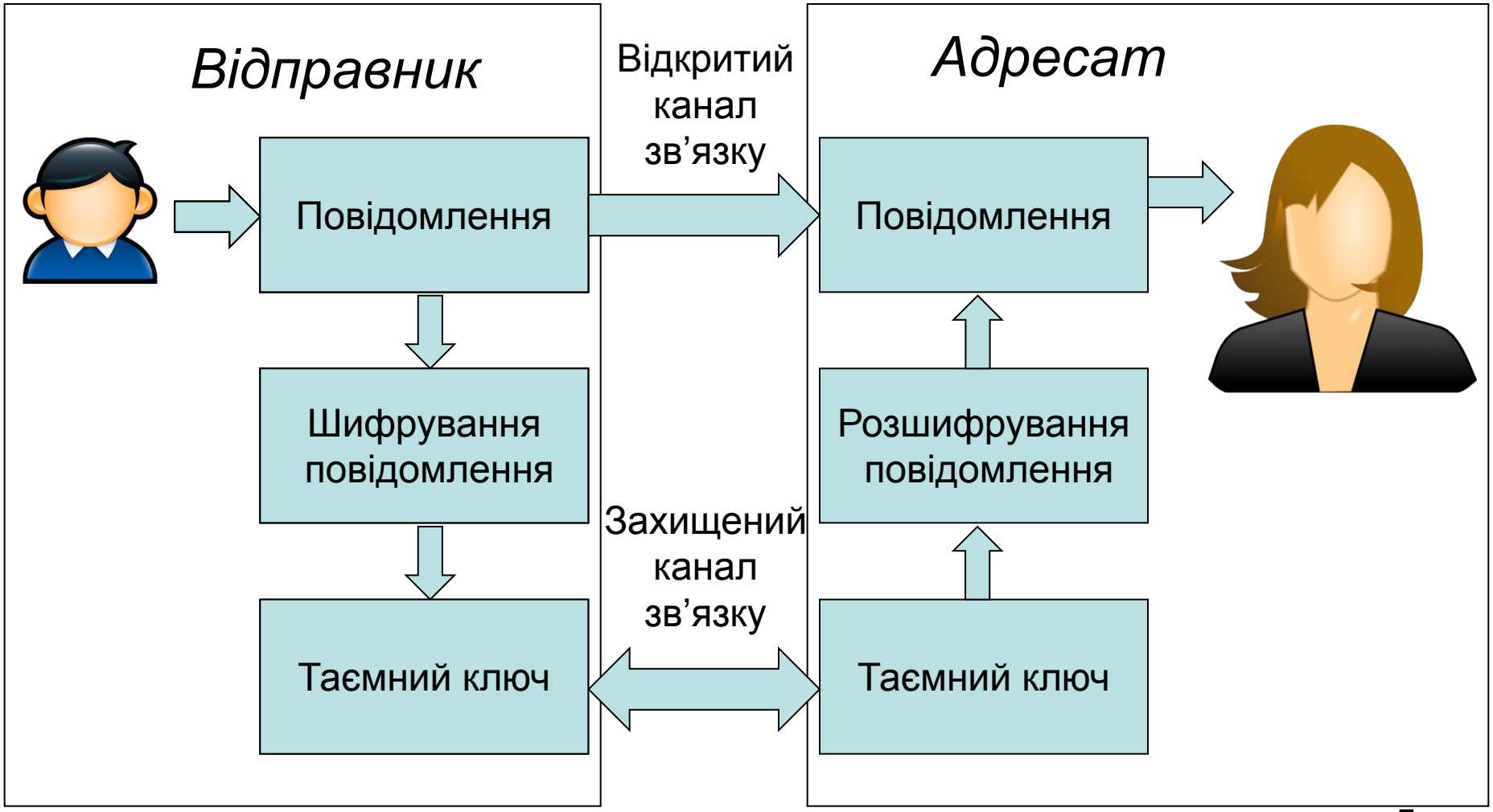
Bombe



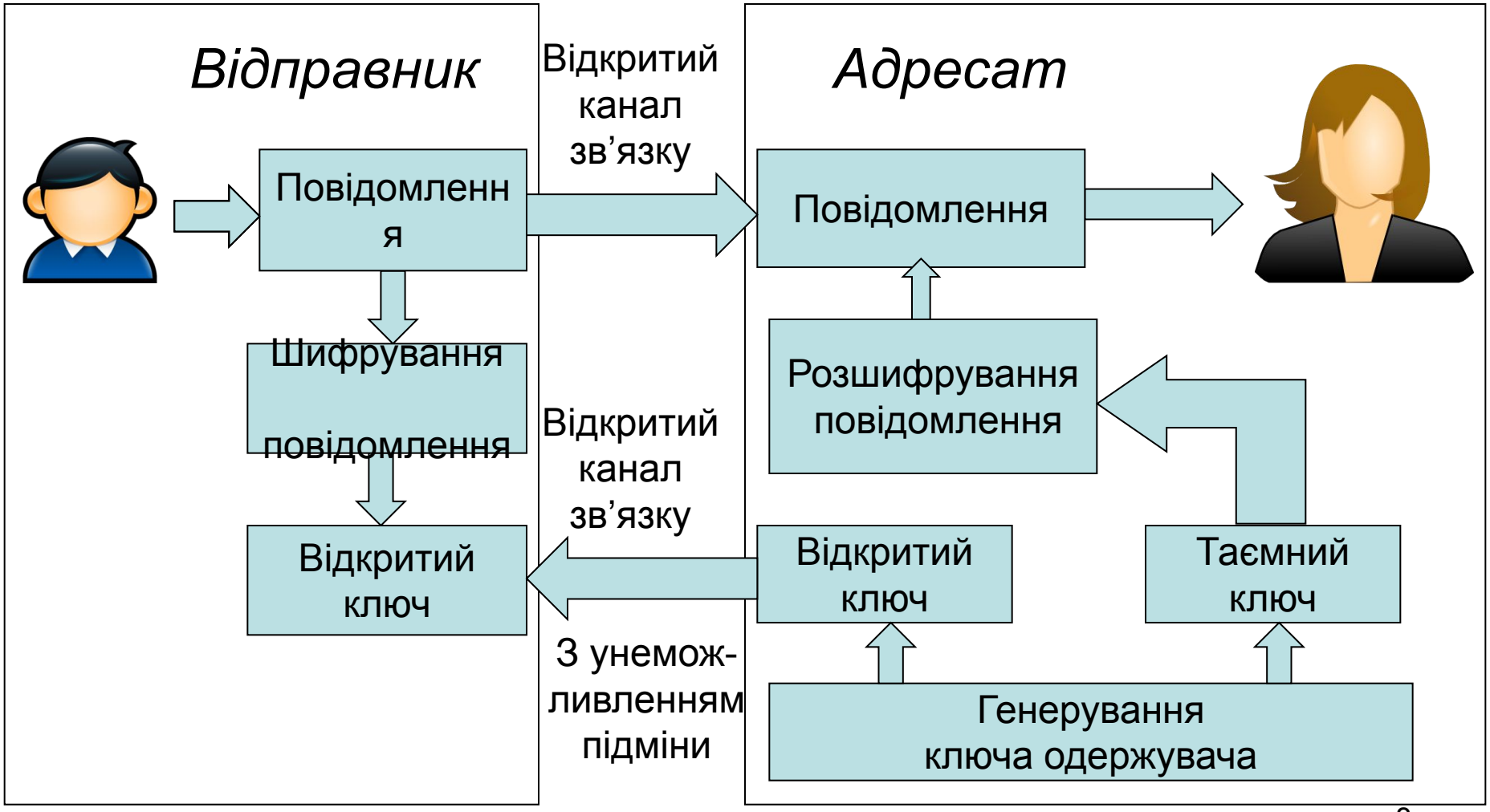
Види шифрування інформації

- Безключові
- *Шифрування з ключем:*
  - *Симетричне шифрування*
  - *Асиметричне шифрування*

Симетричне шифрування (на таємному ключі)



Асиметричне шифрування (на відкритому ключі)



Порівняння симетричного та асиметричного шифрування

Симетричне шифрування	
Переваги	**Недоліки**
• швидкість (на 3 порядки) • простота реалізації • менша довжина ключа для визначення стійкості	• складність управління ключами • складність обміну ключами

Асиметричне шифрування	
Переваги	**Недоліки**
• відсутність необхідності захищеного каналу • наявність тільки одного секретного ключа • число ключів в мережі менше і не росте в квадратичній залежності	• складність проведення зміни алгоритму • неможливість шифрування ID відправника та адресата • велика довжина ключа, порівняно із симетричним шифруванням

Список використаних джерел

- http://www.ixbt.com/soft/alg-encryption.shtml Форум IXBT. Назначение и структура алгоритмов шифрования.
- М.В. Гайоронський, О.М. Новіков Безпека інформаційно-комунікаційних систем — Київ: Видавнича група BHV. 2009,
  — 610 с.
- http://ru.wikipedia.org/wikihttp://ru.wikipedia.org/wiki/http://ru.wikipedia.org/wiki/Криптосистема Криптосистема
- Венбо Мао Современная криптография. Теория и практика — Москва: Вильямс. 2008, — 768 с.
- Панасенко Сергей Алгоритмы шифрования — Санкт-Петербург: БХВ-Петербург. 2009, — 576 с.

Дякую за увагу!

@core_st

core.hor@gmail.com

itblogger.org.ua