Варганова Д. О., ст. викладач кафедри комп'ютерних технологій у медицині та телекомунікаціях
Кукулівський М. О., студент
Державний університет «Житомирська політехніка»

КРИПТОГРАФІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

Останнім часом активно обговорюється проблема захисту інформаційних мереж. Зокрема звертається увага на відсутність своєчасного втручання в випадках, коли надійність передачі даних та їх вміст знаходиться під загрозою. Втручання людини може бути як несвоєчасним, так і неефективним. Також не слід забувати про людський фактор, халатність, некомпетентність персоналу, який може звести нанівець технічний потенціал навіть самих передових систем захисту інформації. Щоб вберегти непосвячену людину від некоректних дій з інформаційними технологіями можна використати вчення про захист інформації, що називається криптографією.

Криптографія – це наука про математичні методи забезпечення конфіденційності, цілісності і автентичності інформації.

Для прикладу пропоную ознайомитися з таблицею заміни для двох шифрів (рис.1).

Відкр. текст	Шифр 1	Шифр 2	Відкр. текст	Шифр 1	Шифр 2	Відкр. текст	Шифр 1	Шифр 2
А	В	^	М	Т	№	Ч	М	∑
Б	И	@	Н	Ц	#	Ш	У	∇
В	О	)	О	.	-	Щ	Д	γ
Г	А	+	П	Ж	=	Ъ	Э	χ
Д	Щ	<	Р	Г	(	Ы	Н	⊕
Е	П	>	С	Л	?	Ь	Ю	×
Ж	К	∀	Т	Х	%	Э	Ы	ω
З	Б	♦	У	С	⊗	Ю	Ш	$
И	Ъ	*	Ф	Ь	!	Я	Е	Δ
К	пробіл	♥	Х	Ч	№	пробіл	Ф	∞
Л	Р	♠	Ц	З	®	.	Я	♣

Рис 1. Таблиця заміни для двох шифрів

Залежно від наявності або відсутності ключа кодовані алгоритми діляться на тайнопис і криптографію. Залежно від відповідності ключів шифрування і дешифрування – на симетричні і асиметричні. Залежно від типу використовуваних перетворень – на підстановочні і перестановочні. Залежно від розміру шифрованого блоку – на потокові та блокові шифри.

Відносно криптоалгоритмів існує кілька схем класифікації, кожна з яких заснована на групі характерних ознак. Таким чиноом, один і той же алгоритм "проходить" відразу за кількома схемами, опиняючись в кожній з них в будь-якій з підгруп. Основною схемою класифікації всіх криптоалгоритмів є наступна:

1. Тайнопис. Відправник і одержувач призводять над повідомленням перетворення, відомі тільки їм двом. Стороннім особам невідомий сам алгоритм шифрування.
2. Криптографія з ключем. Алгоритм впливу на дані, що передаються, котрий відомий всім стороннім особам, але він залежить від деякого параметра – "ключа", яким володіють тільки відправник і одержувач.
3. Симетричні криптоалгоритми. Для кодування і розшифровки повідомлення використовується один і той же блок інформації (ключ).
4. Асиметричні криптоалгоритми. Алгоритм такий, що для шифрування повідомлення використовується один ("відкритий") ключ, відомий всім бажаючим, а для розшифровки – інший ("закритий"), що існує тільки в одержувача.

Робота показує, що протягом усієї своєї історії людству необхідно шифрування тієї чи іншої інформації. З такої потреби виросла ціла наука – криптографія. Раніше криптографія служила тільки інтересам держави, але з появою інтернету її методи стали цікавити і приватних осіб. На сьогоднішній день криптографія широко використовується не лише хакерами, але і борцями за свободу інформації, фінансовим сектором, воєнними структурами та простими користувачами, охочими захистити свої дані в мережі. Актуальність криптографії не згасне в найближчі століття.

Список використаних джерел

1. http://ceit-blog.ucu.edu.ua
2. https://ames.kpi.ua/
https://csecurity.kubg.edu.ua/