Анотація курсу «Основи криптографії»

Програма навчальної дисципліни «Криптографія» складена відповідно до освітньо-наукової програми підготовки першого (освітньо-наукового) рівня вищої освіти (бакалавр). Галузь знань: 10 –“Природничі науки”. Спеціальність: 105 – Прикладна фізика та наноматеріали. Освітньо-наукова програма: “ Прикладна фізика та наноматеріали ”.

Криптологія – це область знань, що вивчає тайнопис (криптографію) і методи її розкриття (криптоаналіз). Побудова сучасної криптології як науки грунтується на сукупності фундаментальних понять математики, фізики, теорії інформації і складності обчислень. Проте, не дивлячись на органічно властиву їй складність, багато теоретичних досягнень криптології, зараз широко використовуються в нашому насиченому інформаційними технологіями житті.

Довгий час криптографія в основному застосовувалася для забезпечення секретності листування в дипломатії, військовій справі, спецслужбами. З розвитком інформаційних технологій застосування криптографічних методів стало актуальним для всього суспільства. Винахід нових принципів криптографії і поява  криптографії з відкритим (або загальнодоступним) ключем дав могутній імпульс для широкого використання криптографії для потреб бізнесу, банківської справи і дозволило забезпечити безпеку взаємодії широкому кругу суб’єктів.

Необхідно розрізняти теоретичну і прикладну криптографію. Для глибокого вивчення питань теоретичної криптографії доводиться знайомитися з теорією вірогідності і статистики, вищою алгеброю, теорією чисел та іншими дисциплінами. Прикладна криптографія більше займається питаннями застосування досягнень теоретичної криптографії для потреб конкретних застосувань на практиці, тобто розробкою криптографічних алгоритмів.

Також необхідно розрізняти теоретичний і практичний криптоаналіз. Основна мета теоретичного криптоаналізу полягає в оцінці стійкості існуючих криптосистем, що розробляються. Оцінка стійкості криптосистем надається у вигляді кількості операцій, необхідних для злому криптосистеми або у вигляді часу, який потрібний для злому. Основна мета практичного криптоаналізу полягає у зломі криптографічних алгоритмів, досліджуючи нові методи і модифікуючи ті, що існують.

Хоча історія криптографії нараховує більш 2000 років, можна вважати, що першою теоретичною роботою можна назвати роботу голландського вченого Керкхоффа, у якій було сформульовано загальноприйняте зараз правило. Воно говорить про те, що стійкість шифру повинна визначатися тільки таємністю ключа. Це означає те, що алгоритм шифрування, текст криптограми відомі криптоаналітику.

Більшість учених уважає, що криптологія як наука виникла після опублікування К.Шенноном статті « Теорія зв'язку в секретних системах» в 1949 році. Перш ніж приступитися до викладу теоретичного матеріалу, викладеного Шенноном у своїй статті, розглянемо сам предмет наших досліджень – криптологічну систему. Сам К.Шеннон використовував термін «секретна система».

Згідно Шеннону, є три загальні типи секретних систем:

1. системи маскування, які включають застосування таких методів, як невидиме чорнило, вистава повідомлення у формі невинного тексту або маскування криптограми, і інші методи, за допомогою яких факт наявності повідомлення ховається від супротивника ( у цей час розробкою засобів і методів приховання фактів передачі повідомлення займається стеганографія);
2. таємні системи (наприклад, інвертування мови), у яких для розкриття повідомлення потрібно спеціальне устаткування;
3. «властиво» секретні системи, де зміст повідомлення ховається за допомогою шифру, коду й т.д.., але саме існування повідомлення не ховається й передбачається, що супротивник має будь-яке спеціальне устаткування, необхідний для перехоплення й запису переданих сигналів.

Роботу криптосистеми найбільш загально можна описати в такий спосіб.

1. Передавальна сторона одержує із джерела ключів ключ для шифрування свого повідомлення.
2. Передавальна сторона зашифровує текст повідомлення й передає криптограму Е в відкритий канал зв'язки в напрямку одержувача.
3. Одержувач повідомлення одержує із джерела ключів ключ, за допомогою якого можна розшифрувати отриману криптограму.
4. Одержувач розшифровує криптограму Е.

На першому етапі розвитку криптології існувало два основних типу перетворень відкритих текстів – заміни й перестановки. Шифрів перестановки відомо достатньо велика кількість – це й шифр «скітала», шифруючи таблиці й ін. Головна ідея шифрів перестановки є заміна місця розташування символів відкритого тексту. Шифрів заміни було значне більше, але всі вони будувалися на заміні символу відкритого тексту символом зашифрованого тексту. До таких шифрів належать полібіанський квадрат, шифруючи таблиці, Трисемуса, система шифрування Віжінера й ін.

На другому етапі передбачалося, що для шифрування й розшифрування використовується один секретний ключ. Дані системи були названі симетричними. Як було сказано вище, основними принципами шифрування стають розсіювання й перемішування. У міру розвитку криптологія в симетричних криптологічгих системах виділяються два головних напрямки шифрування: блокові й потокові шифри. У блокових шифрах відкритий текст розбивається на блоки фіксованої довжини й зазнає шифруванню. Причому кожний блок зашифровується своїм шифром, але алгоритм перемішування залишався однаковим для всіх блоків. На цьому принципі побудовані велика кількість шифрів, включаючи американський стандарт DES і національний стандарт ДЕРЖСТАНДАРТ 28147-89. У блокових шифрах широко використовується перемішування. При використанні потокових

шифрів кожний символ відкритого тексту зашифрується незалежно від інших. Головною проблемою створення потокового шифру є створення послідовності, що шифрує. Вимоги до таких послідовностей досить тверді. Як тільки ми починаємо говорити про шифри, перед нами встає проблема їх передачі до одержувача. При використанні потокових шифрів вони можуть вироблятися як на передавальному, так і на прийомному кінцях лінії зв'язку. У цьому випадку постає проблема синхронізації, і шифри можуть бути синхронні і само синхронні.

Створення персональних ЕОМ відкрило нову сторінку в криптологія. З однієї сторони різко зросли можливості криптоаналітиків. Це в першу чергу стосується криптоаналізу за допомогою простого перебору. З іншої сторони з'явились практично необмежені можливості у шифрувальників, які, використовуючи можливості ПЕОМ, створювати шифри, що практично не розкриваються.