УДК 512.7

Мельник В.Р., здобувач 2 курсу
Половенко Л.П.,доцент
кафедри інформаційних технологій

ЛИШКИ ТА КОДУВАННЯ ПОВІДОМЛЕНЬ

Донецький національний університет імені Василя Стуса

Постановка проблеми: З давніх часів відомо, що одну і ту ж інформацію, наприклад, відомості про небезпеку ми можемо висловити різними способами: просто крикнути; залишити застережливий знак (малюнок); за допомогою міміки та жестів; передати сигнал «SOS», використовуючи азбуку Морзе або семафорну чи прапорцеві сигналізації. У кожному з цих способів ми повинні знати правила, за якими можна відобразити інформацію, щоб отримати та зрозуміти її.Аналіз останніх досліджень: Поняття порівняння, введене Гаусом,знайшло широке застосування в математиці і позначається: a≡b (mod m), де a і b - числа, що дають при діленні на число m (модуль) рівні залишки, і називаються порівнянними за даним модулем.Приклад: 2,9,16 та 23 - порівнянні між собою за модулем 7, бо приділенні кожного числа на 7, виходять залишки, які дорівнюють 2.2≡5 (mod3); 22≡12 (mod5); 1000≡1 (mod37).Знак порівняння «≡» нагадує знак рівності і це не випадково, тому що властивості порівнянь схожі на властивості рівностей.Але поглянувши на порівняння з іншого боку: взявши певний модуль,наприклад, m = 5. При діленні будь-якого числа на 5 вийшли залишки 0,1,2,3 і 4. Всі натуральні числа можна розбити на 5 категорій залежно від того, який залишок виходить при діленні цих чисел на 5. Числа кожної категорії утворюють необмежено-продовжувану арифметичну прогресію.Ось ці п'ять прогресій:

÷1, 6, 11, 16, 21, 26,…
÷2, 7, 12, 17, 22, 27,…
÷3, 8, 13, 18, 23, 28,…
÷4, 9, 14, 19, 24, 29,…
÷5, 10, 15, 20, 25, 30,…

Всі числа, які входять до складу написаних вище прогресій,називаються лишками за модулем 5 (mod 5).Числа такої системи стали додавати, віднімати і множити за звичайними правилами, але кожен отриманий результат замінювати найменшим позитивним лишком того ж класу.Лишки мають різні корисні властивості. Лишки можна використовувати при шифруванні повідомлень. Розглянули найпростішу систему, якою користувався Юлій Цезар. Він застосовував циклічний зсув латинського алфавіту на три літери. Замість «a» він ставив «d», замість «b» ставив «e» і т.д. Замість «x», «y», «z» відповідно «a», «b», «c» Тобто букви

замінені на їхні порядкові номери, які розглядаються за модулем 23 (mod 23),так як в латинському алфавіті 23 літери. Ця ідея заміни символів на відрахування вельми корисна і застосовується в сучасних криптосистемах. Узагальненням системи Цезаря служить Афінна криптосистема. Розглянемо шифрування англійських текстів за допомогою наступного методу. Зіставивши кожній букві англійського алфавіту лишок за модулем 26.Обиремо два числа k и m ($1 \le k \le 25$; $0 \le m \le 25$), причому НОД (k,26)=1.Шифруємо так: лишок замінюється на лишок. Враховуючи, які різні значення можна надати k і m, отримуємо 312 способів шифрування англійських текстів. Однозначно дешифрувати повідомлення можна, якщо відомі k і m (зворотний лишок до лишка).

Висновки. Розглядаючи теорію лишків і кодування можна побачити, що цей розділ математики посідав й посідає дуже важливе місце у житті людини, як в минулому, так і зараз, бо секретність будь-якої важливої інформації можливо зберегти лише за допомогою кодування або шифрування її. Ще не варто забувати, що один з найважливіших винаходів людини - комп`ютер, працює саме через постійне кодування.

Список використаних джерел

1. Берман Г.Н. Число и наука про него / Г.Н. Берман. - М. Государственное издательство технико-теоретической литературы, 1954.-157 с.
2. Илларионова О.Г., Солодов В.В. Комплексные числа, алгебраические структуры / О.Г. Илларионова, В.В.Солодов - М.: МГТУ ГА, 2005. - 24 с.

УДК 004.056.55(043.2)

Мосєвніна А.С.,
здобувач вищої освіти,
Половенко Л.П., доцент, доцент
кафедри прикладної математики

ЕЛЕКТРОННИЙ ПІДПИС: БЕЗПЕКА ТА ЗАХИЩЕНІСТЬ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

В Україні широкого поширення набуло використання електронних документів. Вони не лише існують поряд з традиційними паперовими документами, але все частіше замінюють їх. Цьому сприяють наростаючий темп розвитку цифрових технологій та впровадження на державному рівні проєктів у сфері цифрової трансформації. Легітимним засобом електронної ідентифікації виступає електронний цифровий підпис (ЕЦП). Застосування ЕЦП дозволяє суттєво економити час, необхідний на оформлення