**Лабороторна работа №9**

**Тема:** Хешування з використанням“MD5”

**Мета:** Відпрацювання та закріплення теоретичних відомостей з теми хешування “MD5”

MD5 (Message Digest 5) — 128-бітний алгоритм хешування, розроблений професором Рональдом Л. Рівестом в 1991 році. Призначений для створення «відбитків» або «дайджестів» повідомлень довільної довжини. Прийшов на зміну MD4, що був недосконалим. Описаний в RFC 1321. З 2011 року відповідно RFC 6151 алгоритм вважається ненадійним.

Хешувальними функціями називаються криптографічні перетворення двійкової послідовності довільної довжини у двійкову послідовність кінцевої довжини.

Криптографічні хеш-функції вони повинні бути незворотними. Це означає, що повинно бути обчислювально складно (або взагалі неможливо) за хеш-образом знайти прообраз.

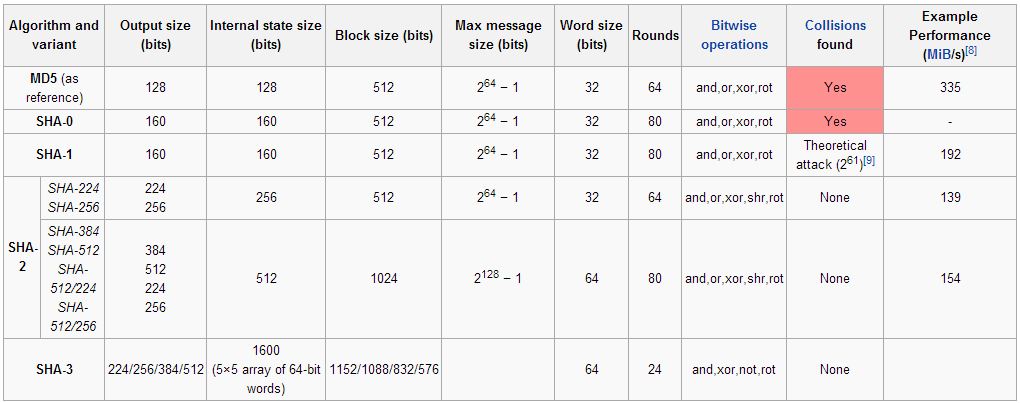
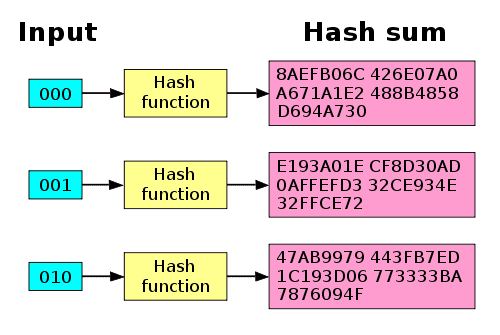


Рисунок . Структура Меркля-Дамгорда

Для того щоб зробити хеш-образ повідомлення **М** за алгоритмом MD5 необхідно зробити:

**Крок 1**. *Доповнення повідомлення*. Оскільки вхідний блок MD5 становить 512 біт, то вхідне повідомлення повинно бути кратним 512 біт.

Доповнюється в такий спосіб:

* Повідомлення доповнюється так, щоб воно було кратним 448 mod 512
* Доповнюється 64-бітами істинної довжини повідомлення;
* Якщо повідомлення більше за 264-1, доповнюється 64 молодшими бітами довжини.
* Повідомлення доповнюється навіть тоді, коли воно вже кратне 512 бітам: треба додати 64 біти довжини. Доповнення відбувається в будь якому випадку.

**Крок 2**. *Ініціалізація буфера*. Ініціалізується чотири 32 бітових регістри А,В,С,D, які заповнюються такими константами зчеплення: шістнадцяткова система

Константи А= 0x01234567; B=0x89abcdef; C=0xfedcba98; D=0x76543210

**Крок 3**. *Обробка повідомлення*. Для обробки повідомлення використовується чотири нелінійні логічні функції:

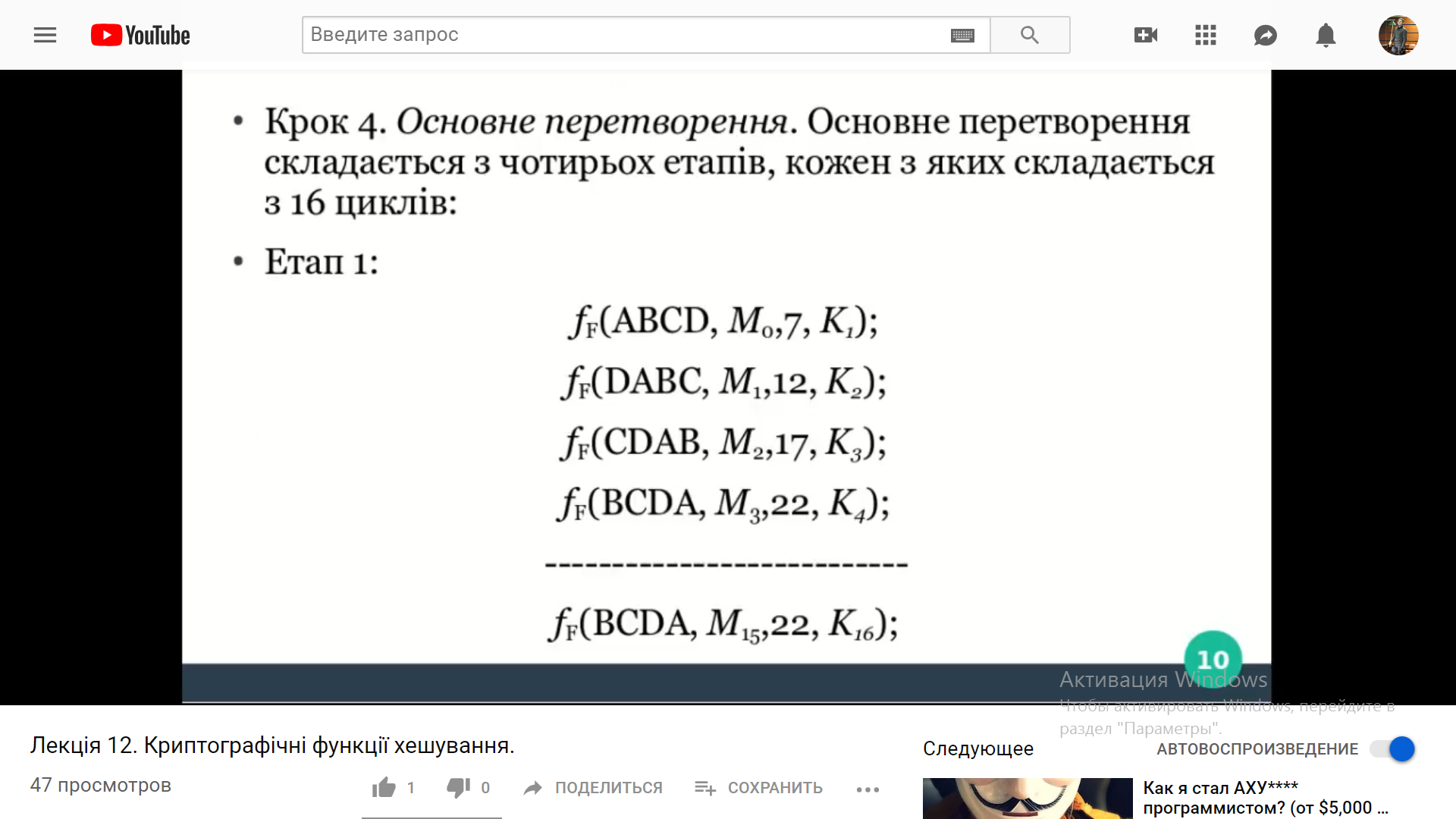
На основі цих функцій створюються процедури обробки тексту.

* підсумовування за модулем ;
* черговий блок тексту;
* циклічний зсув ліворуч на s позицій;
* ціла частина від |sin i|;

Процедури , і будуються аналогічно з використанням решти функцій.

**Крок 4**. *Основне перетворення*. Основне перетворення складається з чотирьох етапів, кожен з яких складається з 16 циклів:

*Етап 1:*



*Етап 2:* Другий етап виконується аналогічно першому, однак замінюється на; замість послідовності 7,12,17,22 використовується 5,9,13,20; замінюється на

*Етап 3:* Аналогічно до попередніх з точністю до процедури (використовується замість ) послідовність зсувів – 4,11,16,23; замість використовують .

*Етап 4:* Аналогічно до попередніх з точністю до процедуру послідовність 6, 10, 15, 21; константи.

**Крок 5**. *Формування хеш-образу*. Після обробки всіх N512-бітових блоків тексту 128-бітоких хеш-образ повідомлення утворюється конкатенацією регістрів A||B||C||D буфера.

**Висновок:**  MD5 можна застосовувати і зараз але не для секретних речей. Оскільки було виявлено наявність існування колізій. Було застосовано досить ефективно метод «Райдужних таблиць» - це атаки на хеш-функції, коли беруться таблиці величезного розміру в яких міститься результати хешування для порівняння та визначення початкового значення інформації, що була захешована. На основі архітектури MD4-MD5 було розроблено хешувальну функцію SHA.

У 2004 році китайські дослідники Сяоюнь Ван (Xiaoyun Wang), Денгуо Фен (Dengguo Feng), Сюецзя Лай (Xuejia Lai) і Хонбо Ю (Hongbo Yu) повідомили про знаходження ними вразливості в алгоритмі, що дозволяє за невеликий час (1 годину на кластері IBM p690) знаходити колізії хеш-функцій.

У 2006 році чеський дослідник Властимил Клима опублікував алгоритм, що дозволяє знаходити колізії з довільним початковим вектором (A,B,C,D) на звичайному комп'ютері за лічені хвилини, Методу було названий «тунелювання».

2009 року підрозділ Національного управління кібербезпеки США US-CERT рекомендував відмовитися від застосування цього алгоритму через виявлені вразливості. Відповідний RFC 6151 було опубліковано в березні 2011 року.