**РЕФЕРАТ**

Два одинарних міжрядкових інтервали

20 мм

Обсяг роботи \_\_ сторінки, \_\_ ілюстрації, \_\_ таблиць, \_\_ додатки, \_\_ джерело літератури.

10 мм

Об’єктом дослідження є………………………………………

25-30 мм

Предметом дослідження є ……………………………………………

шрифтів текстового редактора Wоrd (ТimesNewRoman) розміру 14.

Факторизація, ρ-метод Полларда, графічний процесор

**ABSTRACT**

Першою сторінкою дипломної роботи є титульний аркуш, другою сторінкою – завдання, ці сторінки включаються до загальної нумерації сторінок, але на них номери не проставляються. Наступні сторінки нумерують у правому верхньому куті без крапки в кінці.

**ЗМІСТ**

[Перелік умовних позначень, символів, одиниць, скорочень і термінів 7](#_Toc325014104)

[Вступ 8](#_Toc325014105)

[1 Аналіз методів факторизації 9](#_Toc325014106)

 [1.1 Постановка задачі. Класифікації алгоритмів факторизації 9](#_Toc325014107)

 [1.2 (Р-1) метод Полларда ..10](#_Toc325014108)

 [1.3 Алгоритм факторизації Ленстри на еліптичних кривих 9](#_Toc325014109)

[Висновки до розділу 1 10](#_Toc325014115)2

[2 Ро-метод Полларда. Особливості реалізації для різних моделей обчислень 10](#_Toc325014116)3

[Висновки до розділу 2](#_Toc325014117) 14

[3 Оцінка ефективності методів](#_Toc325014118) 15

 [3.1 Верхня оцінка кількості модулів RSA 16](#_Toc325014119)

[Висновки до розділу 3](#_Toc325014121) 18

[4 Охорона праці та безпека у надзвичайних ситуаціях 20](#_Toc325014122)

 [4.1 Аналіз приміщення 20](#_Toc325014123)

 [4.2 Мікроклімат 21](#_Toc325014124)

 [4.3 Освітлення 22](#_Toc325014125)

[Висновки до розділу 4 27](#_Toc325014130)

[Висновки 28](#_Toc325014131)

[Перелік джерел посилань](#_Toc325014132) 29

[Додаток А (назва) 14](#_Toc325014133)30

# Перелік умовних позначень, символів, одиниць, скорочень і термінів

**Міжрядковий інтервал 1,5**

**Два одинарних міжрядкових інтервали**

*р* | *n* – р ділить n, іншими словами n кратне р;

НСД(*а*,*b*) – найбільший спільний дільник чисел *a*, *b*;

ПЕОМ – персональна електронна обчислювальна машина;

ПК – персональний комп’ютер;

ПЛІС – програмована логічна інтегральна схема;

PGP – Pretty Good Privacy;

**Міжрядковий інтервал 1,5**

MD5 – Message Digest 5;

#

# Вступ

**Два одинарних міжрядкових інтервали**

**20 мм**

**Актуальність роботи…………………………………………………………….**

**Мета і завдання дослідження………………………………………………….**

*Об’єкт дослідження:*…………………………………………………………….

*Предмет дослідження:*……………………………………………………….….

*Метою роботи* є………………………………………………………………….

**Методи дослідження……………………………………………………….……**

**Наукова новизна одержаних результатів…………………………………...**

**Практичне значення одержаних результатів……………………………….**

**Апробація результатів роботи………………………………………………...**

**Публікації……………………………………………………………………..…**

**Все обов’язково висвітлюється у вступі**

# Аналіз методів факторизації

 **без крапки**

|  |
| --- |
|  **Без крапки в кінці** |

**Два одинарних міжрядкових інтервали**

## 1.1 Постановка задачі. Класифікації алгоритмів факторизації

**Два одинарних міжрядкових інтервали**

 **без крапки**

|  |
| --- |
|  **Без крапки в кінці** |

**Нижне поле 20 мм**

## 1.3 Алгоритм факторизації Ленстри на еліптичних кривих



**Міжрядковий інтервал 1,5**

**Ілюстрації позначають словом ”Рисунок” і нумерують послідовно в межах розділу**

Рисунок 1.1 – Розмір дільників, знайдених алгоритмом ECM по роках

**Заголовки підрозділів, пунктів і підпунктів друкують маленькими літерами (крім першої великої), починати з абзацу (5 знаків). Якщо заголовок складається з двох або більше речень, їх розділяють крапкою. Відстань між заголовком та наступним або попереднім текстом має бути не менше 2-х рядків. Не можна розміщувати заголовок у нижній частині сторінки, якщо після нього залишається тільки один рядок тексту.**

**На рівні абзацу**

## 1.4 Числа вигляду $n= p^{r}q$

 **Поле (25 -30 мм) + абзац**

**На рівні абзацу**

## Висновки до розділу 1

**Висновки до розділу можна не починати з нової сторінки.**

#

# 2 РО-метод Полларда. Особливості реалізації для різних моделей обчислень

**Заголовки розділів необхідно розміщувати посередині рядка і друкувати прописними літерами без крапки в кінці.**

**Таблицю розташовують одразу після тексту в якому вона вперше згадується, нумерують послідовно в межах розділу. Поле (25 -30 мм) + абзац**

**Міжрядковий інтервал 1,5**

**На рівні абзацу**

Таблиця 3.1- Класифікація алгоритмів факторизації

|  |  |  |  |
| --- | --- | --- | --- |
| Клас | Назва алгоритму | Складність | Додаткова інформація |
| exp, det | Ферма | $$O\left(n^{c}\right), O(n^{c\_{1}}log^{c\_{2}}n)$$ | *p*і*q* приблизно одного розміру |
| exp, det | (Р-1) Полларда | $$O(n^{1/2}log^{c}n)$$ | Невеликі дільники |
| exp, prob | ρ-Полларда | $$O\left(n^{1/4}\right)$$ | Невеликі дільники |
| exp, det | Шермана-Лемана | $$O\left(n^{1/3}\right)$$ | $$n^{\frac{1}{3}}<p\leq q<n^{\frac{2}{3}}$$ |
| subexp, det | QS | $$L\_{n}[ \frac{1}{2};1]$$ | $$n<10^{110}$$ |

**Таблицю можна перенести на наступну сторінку так:**

 **Поле (25 -30 мм) + абзац**

 Таблиця 5.7 – Характеристики еваковиходів

|  |  |  |
| --- | --- | --- |
| Характеристика | Існуючі значення | Нормативні значення |
| 1 | 2 | 3 |
| Висота дверних прорізів, м**Міжрядковий інтервал 1,5** | 2,32 | не менш 2,0 |
| Продовження (або Кінець)таблиці 5.7 |  |  |
| 1 | 2 | 3 |
| Ширина проходу для евакуації, м | 2,5 | не менш 1,0 |
| Ширина коридору, м | 2,9 | не менш 2,0 |
| Число виходів з коридору | 2 | не менш 2 |

**Поле (25 -30 мм) + абзац**

**Міжрядковий інтервал 1,5**

 (3.1)

де  - математичне очікування;

 – середнє квадратичне відхилення і т.д.;

Формули, що йдуть одна за одною та не розділені текстом, відокремлюють комою. Якщо формула згадується в тексті тільки один раз, її не нумерують.

**перша формула третього розділу**

#  ДОДАТКИ Додаток А

назва