Харківський національний університет радіоелектроніки

Факультет: КІУ Кафедра: Безпеки інформаційних технологій

Спеціальність: 6.1701 “Безпека інформаційних комунікаційних систем”

ЗАТВЕРДЖУЮ
Зав. кафедри БІТ проф. Горбенко І. Д.
“_____” _____ 2012 р.

ЗАВДАННЯ

НА БАКАЛАВРСЬКУ РОБОТУ

Студентові Кіянчуку Руслану Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Аналіз криптографічних властивостей симетричних шифрів
затверджена наказом по університету від "20" 04 2012 р. № 551 СТ
2. Термін здачі студентом закінченої роботи 10.05.2012
Вихідні дані до проекту: наукові публікації з теми роботи.

3. Зміст пояснювальної записки (перелік питань, що їх потрібно розробити)
    1. Сучасний стан аналізу та синтазу симетричних криптографічних перетворень.
    2. Огляд вимог та аналіз властивостей перспективного шифру для компактної реалізації.
    3. Вплив лінійного перетворення на властивості гами шифруючої поточного шифра ZUC.
    4. Алгебраїчний аналіз ГОСТ 28147.
    5. Опис програмної реалізації розроблених методів.
    6. Охорона праці.

4. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, плакатів)
Слайди презентації для захисту роботи
5. Матеріали, що заборонені до відкритого оголошення та їх гриф
Відсутні

6. Основна література та джерела

    1. Martin Albrecht. Algebraic Attacks on the Courtois Toy Cipher, 2006. – Режим доступа: www/URL: http://www.sagemath.org/files/thesis/albrecht-thesis-2006.pdf.
    2. Gregory V. Bard. Algebraic Cryptanalysis. – Springer Science & Business Media, 2009, ISBN 9781441910196. – Режим доступа: www/URL: http://books.google.com.ua/books?id=PYs4Vjdo0z0C.
    3. Stein W. A. et al. — Sage Mathematics Software (Version 4.8). — The Sage Development Team, 2012. . – Режим доступа: www/URL: http://www.sagemath.org./
    4. A. Bogdanov and L.R. Knudsen and G. Leander and C. Paar and A. Poschmann and M.J.B. Robshaw and Y. Seurin and and C. Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher // Proceedings of CHES 2007. — Springer-Verlag, 2007.
    5. Specification of the 3GPP Confidentiality and Integrity Algorithms 128- EEA3 & 128-EIA3. Document 2: ZUC Specification : Rep. / 3GPP ; Executor: ETSI/SAGE Task Force : 2011. — Version: 1.6.

7. Консультанти з роботи із зазначенням розділів роботи, що їх стосуються

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Спец. частина	доц. Олійников Р. В.		
ОП	ст. викл. Стиценко Т. Є.		

8. Дата видачі завдання 25.02.2012

Керівник роботи _____ доц. Халімов Г. З.
(підпис) (посада, прізвище, ім'я, по батькові)

Завдання прийняв до виконання _____
(підпис студента-дипломника)

КАЛЕНДАРНИЙ ПЛАН

Номер	Назва етапів дипломної роботи	Термін виконання етапів роботи	Примітка
1.	Аналіз літературних джерел	25.02.2012	
2.	Дослідження сучасного стану симетричних криптографічних перетворень	03.03.2012	
3.	Аналіз властивостей перспективного шифру для компактної реалізації	07.03.2012	
4.	Дослідження впливу лінійного перетворення на властивості гами шифруючої шифра ZUC	15.03.2012	
5.	Розробка програмної реалізації методів алгебраїчного криптоаналізу	05.04.2012	
6.	Алгебраїчний аналіз ГОСТ 28147	20.04.2012	
7.	Оформлення пояснювальної записки	05.05.2012	

Студент _____
(підпис)

Керівник роботи _____
(підпис)