Список тем курсовых работ

проф. А.С.Андреев.

По дисциплине «Криптографические методы защиты информации»

1.Схемы разделения секрета на основе китайской теоремы об остатках.

2. Реализация алгоритма Дормана-Принса 7(8).

3. Разложение на множители при помощи эллиптических кривых.

Литература.

1. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — Москва : Издательство Юрайт, 2019. — 309 с. — (Высшее образование). — ISBN 978-5-534-02574-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/433133
2. Рацеев С.М. Математические методы защиты информации : электронный учебный курс / С. М .Рацеев; УлГУ, ФМИАТ. - Ульяновск :УлГУ, 2018. — URL: http://edu.ulsu.ru/cources/921/interface
3. Аминаров А. В. Лабораторный практикум по математическим методам защиты инфор-мации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск :УлГУ, 2016. 55 с. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/270
4. Рацеев С.М. Лабораторный практикум по криптографическим протоколам / С. М. Рацеев; УлГУ, ФМИАТ, Каф. информ. безопасности и теории управления. - Улья-новск :УлГУ, 2019. - URL: http://lib.ulsu.ru/MegaPro/Download/MObject/1344
5. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисци-плине «Криптографические протоколы» для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск :УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 128 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4686
6. ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:

6.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защитаинформации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012

6.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защитаинформации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012

7. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

По дисциплине «Криптографические протоколы и стандарты»

1.Шифрование в аналоговой телефонии.

2.Схемы предварительного распределения ключей в сети связи.

Литература.

1. Зубов А.Ю. Криптографические методы защиты информации. Совершенные шифры. М.: Гелиос АРВ, 2005. 192 с.
2. Рацеев С.М. Математические методы защиты информации : электронный учебный курс /С. М. Рацеев; УлГУ, ФМИАТ. - Ульяновск :УлГУ, 2018. — URL: http://edu.ulsu.ru/cources/921/interface

3.ГОСТ-Эксперт – единая база ГОСТов Российской Федерации для образования и промышленности:
3.1. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защитаинформации. Процессы формирования и проверки электронной цифровой подписи. М.: Стандартинформ, 2012. — URL: https://gostexpert.ru/gost/gost-34.10-2012
3.2. ГОСТ Р 34.11-2012. Информационная технология. Криптографическая защитаинформации. Функция хэширования. М.: Стандартинформ, 2013. — URL: https://gostexpert.ru/gost/gost-34.11-2012
4. Аминаров А. В. Лабораторный практикум по математическим методам защиты информации : учеб.-метод. указания для спец. "Компьютерная безопасность, "Математическое обеспечение и администрирование информационных систем" / А. В. Аминаров, А. М. Иванцов, С. М. Рацеев. Ульяновск :УлГУ, 2016. 55 с. -URL: http://lib.ulsu.ru/MegaPro/Download/MObject/270
5. Рацеев С. М. Методические указания для самостоятельной работы студентов по дисциплине «Криптографические методы защиты информации» для студентов специальности 10.05.01 «Компьютерная безопасность» / С. М. Рацеев; УлГУ, Фак. математики, информ. и авиац. технологий. - Ульяновск :УлГУ, 2019. - Загл. с экрана; Неопубликованный ресурс. - Электрон. текстовые дан. (1 файл : 181 КБ). - Текст : электронный. Режим доступа: http://lib.ulsu.ru/MegaPro/Download/MObject/4685
6. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» / А.С. Андреев, А.М. Иванцов, С.М. Рацеев.– Ульяновск: УлГУ, 2017. – 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.