БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_1\_**

Дисциплина Теория Информации

1. Бинарный алгоритм.
2. Генераторы нелинейных М-последовательностей.
3. Алгоритм цифровой подписи DSA.
4. Основные положения эллиптической криптографии. Эллиптические группы.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_2\_**

Дисциплина Теория Информации

1. Введение. Криптографическое преобразование информации.
2. Сравнения. Модулярная арифметика.
3. Графическая стеганография. LSB стеганография.
4. Эллиптические кривые. Свойства. Аналитические соотношения.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_3\_**

Дисциплина Теория Информации

1. Классический информационный канал. Формальное описание криптосистемы.
2. BPCS стеганография.
3. Комбинированные генераторы ключа. Генератор «Stop and Go».
4. Лексическая стеганография.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_4\_**

Дисциплина Теория Информации

1. Требования к криптографической системе. Требования секретности и достоверности. Классификация криптосистем.
2. Графическая стеганография. Run-Length механизм.
3. Комбинированные генераторы ключа. Каскадный генератор Gollmann.
4. Потоковая криптосистема А5/1.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_5\_**

Дисциплина Теория Информации

1. Криптосистемы с открытым ключом. Характеристика подобных систем.
2. Алгоритм цифровой подписи ElGamal.
3. Комбинированные генераторы ключа. Пороговый генератор.
4. Открытая система распределения ключей (Алгоритм Diffie, Hellman).

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_6\_**

Дисциплина Теория Информации

1. Алгоритмы шифрования: Перестановочные шифры.
2. Способы решения линейных cравнений: 1 случай (нет решений).
3. Самосинхронизирующиеся потоковые криптосистемы.
4. Эллиптические группы. Порядок точки эллиптической группы.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_7\_**

Дисциплина Теория Информации

1. Алгоритмы шифрования: Алгоритм вращающихся квадратов.
2. Способы решения линейных сравнений: 2 случай (одно решение).
3. Функция Эйлера.
4. Эллиптическая криптосистема.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_8\_**

Дисциплина Теория Информации

1. Алгоритмы шифрования: Подстановочные шифры. Алгоритм Цезаря.
2. Способы решения линейных сравнений: 3 случай (множество решений).
3. Экспоненциальный шифратор (Pholing & Hellman).
4. Распределение ключей (симметричные криптосистемы).

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_9\_**

Дисциплина Теория Информации

1. Алгоритмы шифрования: Алгоритм децимации. Аффинное преобразование.
2. Симметричные криптосистемы. Lucifer. DES.
3. Шифратор на базе таблиц Порта. Шифратор Виженера.
4. Алгоритм обмена ключами по открытому каналу с использованием эллиптических групп.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_10\_**

Дисциплина Теория Информации

1. Шифраторы, использующие различные алфавиты. Шифр церковного двора.
2. CPT схема. (Графическая стеганография).
3. Криптосистема типа «рюкзак» №3.
4. Протокол распределения ключей для асимметричных алгоритмов.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_11\_**

Дисциплина Теория Информации

1. DES: получение итерационных ключей.
2. Модификация криптосистемы типа «рюкзак» до криптосистемы с открытым ключом.
3. Квантовая криптография принцип неопределенности Гейзенберга. Квантовая теорема неклонируемости.
4. Гомофонные шифраторы (Омофонные шифраторы).

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_12\_**

Дисциплина Теория Информации

1. Шифратор Билла (Beale).
2. Международный алгоритм шифрования данных (IDEA). Основные характеристики и операции.
3. Электронная цифровая подпись на основе RSA.
4. Протокол ВВ84. Пример реализации протокола.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_13\_**

Дисциплина Теория Информации

1. Шифратор Playfair.
2. Алгоритм BlowFish. Процесс инициализации P-массивов и S-матриц. Структура алгоритма.
3. Потоковые системы шифрования.
4. Атаки на квантовые криптосистемы (Man in the Middle).

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_14\_**

Дисциплина Теория Информации

1. Расщепленный шифр. Bifid шифр.
2. Процедура коррекции сырого ключа в ВВ84. Протокол Беннета.
3. Алгоритм Blowfish. Функция F алгоритма. Достоинства.
4. Физическая криптография. Физически неклонируемые односторонние функции. PUF типа Arbitr.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_15\_**

Дисциплина Теория Информации

1. Шифры, использующие коды переменной длины на примере VIC-шифратора.
2. Цифровая подпись, основанная на симметричных алгоритмах. (ЭЦП Matyas & Meyer)
3. PUF типа Кольцевой осциллятор (Ring Oscilator).
4. ABCDE стеганография.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_16\_**

Дисциплина Теория Информации

1. Современная роторная машина.
2. Регистры сдвига с линейной обратной связью двух типов.
3. Однонаправленные хэш-функции. Основные свойства.
4. Графическая стеганография Patchwork метод.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_17\_**

Дисциплина Теория Информации

1. Криптосистема RSA.
2. Свойства М-последовательностей.
3. Элементы математических основ криптографии. Количество информации. Энтропия.
4. PUF на базе статических запоминающих устройств.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_18\_**

Дисциплина Теория Информации

1. Симметричные криптосистемы. Lucifer.

1. Пример потоковой криптосистемы на базе М-последовательностей.
2. Скорость языка.
3. Слепая подпись.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_19\_**

Дисциплина Теория Информации

1. Введение в теорию чисел. Теорема Евклида. Теорема 2. Теорема 3.
2. Недостаток синхронных потоковых криптосистем. Процедура их взлома.
3. SHA хэш алгоритм.
4. Обфускация (Obfuscation). Лексическая обфускация.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_20\_**

Дисциплина Теория Информации

1. Алгоритм Евклида.
2. Текстовая стеганография.
3. Иерархия криптографических ключей. Методы генерирования ключей.
4. Генераторы криптографического ключа для потоковых криптосистем. Генераторы М-последовательностей. Достоинства и недостатки.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_21\_**

Дисциплина Теория Информации

1. Последовательность Форда.

2. Генерирование простых чисел. Решето Эратосфена.

3. Отличия между потоковыми и классическими симметричными криптосистемами.

4. Вычисление мультипликативной инверсной величины.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_22\_**

Дисциплина Теория Информации

1. Генератор последовательностей de Bruin.
2. Стеганография (Общая информация).
3. Абсолютная секретность.
4. Управление ключами. Деление ключей.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_23\_**

Дисциплина Теория Информации

1. Стеганография, основанная на формальных грамматиках (Mimicry).
2. Комбинированные генераторы ключа. Генератор Geffe.
3. Теорема Ферма.
4. Обфускация данных.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_24\_**

Дисциплина Теория Информации

1. Аутентификация ключей.
2. Потоковая криптосистема RC 4.
3. Обфускация управления выполнения программы (Control Flow)
4. DES: функция f, реализующая подстановку.

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

**Экзаменационный билет №\_25\_**

Дисциплина Теория Информации

1. Роторные машины. Структура роторной машины.
2. Криптосистема типа рюкзак №1 и №2.
3. Международный алгоритм шифрования данных (IDEA): структуры одного из раундов, получение итерационных ключей.
4. Цифровая подпись. Цифровая подпись, основанная на симметричных алгоритмах.(ЭЦП Diffie & Lamport).

Зимняя экзаменационная сессия 2018-2019 учебного года.

Зав. каф.\_\_\_\_\_\_\_\_\_ Н.В. Лапицкая Преподаватель \_\_\_\_\_\_\_\_\_\_\_В.Н. Ярмолик

Дата утверждения 15.11.2018