

# Оглавление

Введение .....	3
<b>1. Классическая криптография с открытым ключом .....</b>	<b>8</b>
1.1. Основные определения современной криптографии .....	8
1.2. Схемы асимметричной криптографией .....	15
1.2.1. Криптосистема RSA .....	18
1.2.2. Ключевые системы и алгоритм Диффи–Хеллмана .....	19
1.2.3. Криптосистема Эль-Гамала .....	27
1.2.4. Криптосистемы, основанные на эллиптических кривых .....	27
1.2.5. Схема электронной подписи ГОСТ 34.10-2018 .....	30
Контрольные вопросы по разделу 1 .....	37
<b>2. Оценка квантовой устойчивости используемых в различных сферах телекоммуникационной инфраструктуры криптографических алгоритмов .....</b>	<b>38</b>
2.1. Безопасность транспортного уровня .....	41
2.2. PKI и приложения для цифровых сертификатов .....	47
2.3. Электронные подписи .....	50
2.4. Безопасность сети Wi-Fi .....	52
2.5. Безопасность используемых операционных систем .....	53
2.6. Криптовалюты и блокчейн .....	54
2.7. Bluetooth, NFC, IoT и аппаратные устройства .....	57
2.8. Специфика использования криптографии с открытым ключом в России .....	58
Контрольные вопросы по разделу 2 .....	62
<b>3. Общие подходы к построению постквантовых алгоритмов криптографии .....</b>	<b>63</b>
3.1. Основные подходы к построению квантово-устойчивых алгоритмов .....	64

3.2. Постквантовые алгоритмы, основанные на использовании групп кос .....	67
3.3. Постквантовые алгоритмы, основанные на использовании протоколов нулевого разглашения .....	77
3.4. Конкурс NIST PQS и мировой опыт стандартизации .....	87
Контрольные вопросы по разделу 3 .....	96
<b>4. Постквантовые алгоритмы, основанные на теории целочисленных решеток .....</b>	<b>97</b>
4.1. Вычислительно сложные задачи в теории решеток .....	102
4.2. Схема шифрования GGH .....	105
4.3. Схема шифрования NTRU .....	107
4.4. Схема электронной подписи Falcon .....	114
Контрольные вопросы по разделу 4 .....	119
<b>5. Постквантовые алгоритмы, основанные на кодах, исправляющих ошибки .....</b>	<b>120</b>
5.1. Шифрсистема Мак-Элиса .....	126
5.2. Шифрсистема Нидеррайтера .....	128
5.3. Коды, используемые в шифрсистемах .....	130
5.4. Некоторые модификации шифрсистем Мак-Элиса и Нидеррайтера .....	133
5.5. Схемы симметричного шифрования и электронной подписи .....	138
5.6. Алгоритмы, основанные на кодах, на конкурсе NIST .....	141
Контрольные вопросы по разделу 5 .....	145
<b>6. Постквантовые алгоритмы, основанные на многочленах от многих переменных .....</b>	<b>146</b>
6.1. Общие принципы построения алгоритмов типа МРКС .....	148
6.2. Шифрсистема Мацумото–Имаи .....	152
6.3. NFE-алгоритмы и их модификации .....	154
6.4. Системы на основе уравнений с «масляно-уксусным» разделением переменных .....	159
6.5. Модификации UOV-схем .....	161
Контрольные вопросы по разделу 6 .....	167
<b>7. Постквантовые алгоритмы, основанные на криптографических хеш-функциях .....</b>	<b>168</b>

---

7.1. Схема Лампорта (L-OTS).....	174
7.2. Подпись Меркла (MSS) .....	176
7.3. Расширенная подпись Меркла (XMSS) .....	180
7.4. Подпись SPHINCS+ .....	184
Контрольные вопросы по разделу 7 .....	192
<b>8. Постквантовые алгоритмы, основанные на использовании изогений на суперсингулярных эллиптических кривых .....</b>	<b>193</b>
8.1. Основные определения и примеры .....	195
8.2. Протоколы согласования ключей на суперсингулярных изогениях (SIDH и SIKE) .....	205
8.3. Схема электронной подписи на суперсингулярных изогениях .....	212
Контрольные вопросы по разделу 8 .....	215
Приложение. Математические основы криптографии ...	216
Литература .....	222