Задания заключительного по направлению «Безопасность информационных систем и технологий критически важных объектов»

Категория участия: «Бакалавриат»

Теоретическая часть

Номер задания	Задание	Макс. кол-во баллов
Раздел 1. «Математические методы защиты информации»		
1.	Ярослав решил в качестве подстановки S-блока своего блочного шифра выбрать преобразование над полем Галуа $\mathbb{F}_{2^4}$, заданное условием $s_j: x \to x^j$ для каждого $x \in \mathbb{F}_{2^4}$, где $j \in \{1, \dots, 15\}$. Поле $\mathbb{F}_{2^4}$ порождено неприводимым многочленом $x^4 + x^3 + 1$. 1) Если j случайно выбирается из множества {1,…,15}, то с какой вероятностью s_j является подстановкой? 2) Для каждой подстановки s_j выписать все неподвижные точки. Если $j \in \{1, \dots, 15\}$ таково, что s_j не является подстановкой, то s_j не рассматривается. **Ответ:** **1) $8/15$;** **2) каждая подстановка s_j имеет две неподвижные точки $0, 1$.**	5
2.	Алисе задали большое домашнее задание по курсу «Теоретико-числовые методы криптографии». В одном из заданий ей требуется проверить на разрешимость 10 сравнений первой степени: $75025x \equiv 46368 \bmod 121393$ $4181x \equiv 2584 \bmod 6765$ $233x \equiv 144 \bmod 377$ $196418x \equiv 121393 \bmod 317811$ $610x \equiv 377 \bmod 987$ $89x \equiv 55 \bmod 144$ $28657x \equiv 17711 \bmod 46368$ $10946x \equiv 6765 \bmod 17711$ $514229x \equiv 317811 \bmod 832040$ $1597x \equiv 987 \bmod 2584$ Сколько раз Алисе придется делить с остатком, чтобы решить задание с использованием алгоритма Евклида? **Ответ: 200**	4
3.	Криптоаналитик разработал атаку на алгоритм блочного шифрования по известным открытым текстам. Алгоритм атаки принимает на вход по одному блоку открытого текста и шифртекста и завершается успешно с вероятностью p. Какое число пар блоков открытого текста и шифртекста необходимо для успешного выполнения атаки с вероятностью p^*? Успешность выполнения атаки для разных пар открытого текста и	4

	шифртекста считать независимыми. Параметры: p=0,3; p*=0,9. **Ответ: 7**	
4.	Шифрование осуществляется на алфавите «А,Б,В,Г,Д,Е,Ж,З». Алгоритм шифрования определяется как $s^{-1}as(x)$, где s – подстановка на алфавите, $a(b_i) = b_{i+2 \bmod 8}$ для $i = 0, \dots, 7$, где $b_i -$ -я буква алфавита, нумерация букв алфавита с нуля. Подстановка s записана в виде произведения независимых циклов s = (А, Ж, З, Б, Г, В , Е, Д) (т.е. s(А)=Ж). Дан шифртекст «ЕГАЗДВД». Найти открытый текст. **Ответ: ГДЕЖАБА**	4
Раздел 2. «Прикладная криптография»		
5.	Для реализации программного шифратора использовалась реализация OpenSSL на основе отечественных криптоалгоритмов gost-engine. Исходный код представлен в Листинге ниже. ```c // gcc gost89.c olym_encryptor.c -lssl -lcrypto -o olym_enc #include <stdlib.h> #include <string.h> #include <unistd.h> #include <openssl/conf.h> #include <openssl/crypto.h> #include <openssl/engine.h> #include <openssl/evp.h> #include <openssl/hmac.h> #include <openssl/obj_mac.h> #include "gost89.h" #define G89_MAX_TC_LEN (2048) #define G89_BLOCK_LEN (8) const byte key[EVP_MAX_KEY_LENGTH] = { 0x54, 0x6d, 0x20, 0x33, 0x68, 0x65, 0x6c, 0x32, 0x69, 0x73, 0x65, 0x20, 0x73, 0x73, 0x6e, 0x62, 0x20, 0x61, 0x67, 0x79, 0x69, 0x67, 0x74, 0x74, 0x73, 0x65, 0x68, 0x65, 0x20, 0x2c, 0x3d, 0x73 }; const byte iv[EVP_MAX_IV_LENGTH] = {0}; gost_subst_block sbox = { {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07, 0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f}, {0x10, 0x11, 0x12, 0x13, 0x14, 0x15, 0x16, 0x17, 0x18, 0x19, 0x1a, 0x1b, 0x1c, 0x1d, 0x1e, 0x1f}, {0x20, 0x21, 0x22, 0x23, 0x24, 0x25, 0x26, 0x27, 0x28, 0x29, 0x2a, 0x2b, 0x2c, 0x2d, 0x2e, 0x2f}, {0x30, 0x31, 0x32, 0x33, 0x34, 0x35, 0x36, 0x37, 0x38, 0x39, 0x3a, 0x3b, 0x3c, 0x3d, 0x3e, 0x3f}, {0x40, 0x41, 0x42, 0x43, 0x44, 0x45, 0x46, 0x47, 0x48, 0x49, 0x4a, 0x4b, 0x4c, 0x4d, 0x4e, 0x4f}, {0x50, 0x51, 0x52, 0x53, 0x54, 0x55, 0x56, 0x57, 0x58, 0x59, 0x5a, 0x5b, 0x5c, 0x5d, 0x5e, 0x5f}, {0x60, 0x61, 0x62, 0x63, 0x64, 0x65, 0x66, 0x67, 0x68, 0x69, 0x6a, 0x6b, 0x6c, 0x6d, 0x6e, 0x6f}, {0x70, 0x71, 0x72, 0x73, 0x74, 0x75, 0x76, 0x77, 0x78, 0x79, 0x7a, 0x7b, 0x7c, 0x7d, 0x7e, 0x7f}, }; typedef enum g89_mode_ { G89_ECB, G89_CFB, G89_CNT, G89_IMIT } g89_mode; void usage(){ fprintf(stderr, "~~~ OLYMP GOST ENCRYPTOR ~~~\n"); fprintf(stderr, "./olymp_enc <enc mode> <in> <out>\n"); exit(0); }	4

	`` void enc(gost_ctx* ctx, char *in, char *out, size_t in_size, g89_mode mode){ switch(mode) { case G89_ECB: gost_enc(ctx, in, out, (int)((in_size + G89_BLOCK_LEN - 1) / G89_BLOCK_LEN)); break; case G89_CFB: gost_enc_cfb(ctx, (char*)&iv, in, out, (int)((in_size + G89_BLOCK_LEN - 1) / G89_BLOCK_LEN)); break; } } int main(int argc, char**argv){ int err = -1; int rbytes = 0; gost_ctx ctx = {0}; char in[0x1000] = {0}; char out[0x1000] = {0}; const gost_subst_block *pSubst = &sbox; if (argc < 2){ usage(); } g89_mode mode = atoi(argv[1]); gost_init(&ctx, pSubst); gost_key(&ctx, (char*)&key); if (argc < 3){ do { rbytes = read(0, &in, sizeof(in)); enc(&ctx, (char*)&in, (char*)&out, rbytes, mode); write(1, out, rbytes); } while (err != -1); } else if (argc == 4) { fprintf(stderr, "not implemented\n"); usage(); } else { usage(); } } ``` Опишите возможные положительные и отрицательные свойства реализованного программного криптографического средства.	
Решение	Положительные свойства: • Высокая производительность шифратора Отрицательные свойства: • Отсутствие выравнивания блоков открытого текста, что может приводить к программным ошибкам, таким как утечка памяти • Выбранные `sbox` подстановки в слое нелинейной замены отличны от стандарта и имеют простой вид – последовательность чисел от 0 до 0x7F • Вектор инициализации `IV` имеет нулевое значение и не меняется для различных открытых текстов • Ключ шифрования не меняется для различных открытых текстов • Отсутствуют флаги оптимизации при компиляции шифратора	
6.	X – аддитивная группа. Верно ли, что для любой последовательности $\{x_i\}$ над X и для любого натурального числа t существует последовательность $\{y_i\}$ над X, для которой длина периода последовательности $\{x_i + y_i\}$ равна t?	4
Решение	Рассмотрим последовательность $\{z_i\}$ с периодом t. Такую последовательность всегда можно построить над любой аддитивной группой X. Отметим, что для любой последовательности $\{x_i\}$ будет существовать	

	обратная ей последовательность $\{-x_i\}$, так как в группе у любого элемента существует обратный. Тогда сможем построить последовательность $\{z_i - x_i\} = \{y_i\}$. Заметим, что $\{z_i\} = \{x_i + y_i\}$, при этом периоды последовательностей $\{z_i\}$ и $= \{x_i + y_i\}$ также совпадают. Значит, $\forall \{x_i\}$ над X и $\forall\, t \in N \;\; \exists \{y_i\}$ над X: $t(\{x_i + y_i\}) = t$, что и требовалось доказать	
7.	Согласно RFC8446, протокол TLSv1.3 имеет вид, представленный в Листинге ниже. Client Server Key ^ ClientHello Exch | + key_share* | + signature_algorithms* | + psk_key_exchange_modes* v + pre_shared_key* --------> ServerHello ^ Key + key_share* | Exch + pre_shared_key* v {EncryptedExtensions} ^ Server {CertificateRequest*} v Params {Certificate*} ^ {CertificateVerify*} | Auth {Finished} v <-------- [Application Data*] ^ {Certificate*} Auth | {CertificateVerify*} v {Finished} --------> [Application Data] <-------> [Application Data] Имеется сеть с общающимися абонентами, при этом известно, что: • Абоненты используют заранее согласованные ключи шифрования • Не требуется аутентификация клиента и сервера • Идентификаторы секретных ключей можно отправить в открытом виде Исходя из вышеописанных утверждений, определить, какие пакеты будут являться избыточными для описанной сети в приведенной схеме TLSv1.3.	4
Решение	Лишние сообщения: • Сообщения `key_share` у сервера клиента, так как абоненты используют заранее согласованные секретные ключи • Сообщение `psk_key_exchange_modes`, так как идентификаторы секретных ключей передаются в открытом виде • Сообщения с префиксом `Certificate..`, так как не требуется аутентификация абонентов •	
8.	Алиса и Боб используют анонимный протокол Диффи-Хеллмана для формирования общего секрета. Далее они используют выработанный секрет в качестве ключа шифрования симметричного блочного шифра. Какие возможные недостатки использования данной схемы? Предложить как минимум две различных атаки на данную схему и способы защиты от них.	4
Решение	Можно отметить следующие недостатки: • Существует возможность провести атаку типа «человек посередине». Необходимо добавить аутентификацию сторон и подписывать отправляемую сторонами информацию.	

	• Использование непосредственно выработанного секрета в протоколе Диффи-Хеллмана в качестве ключа шифрования небезопасно Ключ должен представлять собой имитацию равномерно распределенной случайной последовательности, где каждый бит появляется с вероятностью 0.5. Выработанный секрет, g^{ab} является случайным элементом математической группы, а не случайной двоичной последовательностью, так как биты числа g^{ab} могут иметь статистическое смещение. К примеру, в случае мультипликативной группы $Z13$ с порождающим элементом g = 2 при случайном выборе показателя степени g будет получен случайный элемент из Z13. Однако представление элемента из Z13 в качестве битовой строки длиной 4 распределено неравномерно: у элементов от 1 до 7 старшим битом является 0, у элементов от 8 до 12 старшим битом является 1. То есть вероятность того, что старший бит равен 0, равна ≈ 0.58, а не требуемые 0.5. Для выработки общего ключа шифрования необходимо преобразовать полученный секрет с помощью стойкой хэш-функции, к примеру SHA-3, либо с помощью функции формирования ключа, к примеру HKDF.	
Раздел 3. «Безопасность информационных технологий и техническая защита информации»		
9.	C/C++ char *CUT_CramMd5::GetClientResponse(LPCSTR ServerChallenge) { ... if (m_szPassword != NULL) { ... if (m_szPassword != '\0') { ... } Выполните описание уязвимости и дайте рекомендации по её устранению	3
Решение	В приведенном примере происходит проверка неравенства указателя на пароль значению «NULL» и что строка не пустая. Вместо этого два раза проверяется неравенство указателя «NULL». Проверка, что строка пустая, не работает. Вызов «m_szPassword != '\0'» необходимо заменить на «*m_szPassword != '\0'».	
10.	При проведении лабораторных измерений в вибрационном канале утечки информации были получены следующие результаты: - уровень вибрационного шума в 1-ой октаве:Vш1 =80дБ; - уровень вибрационного шума во 2-ой октаве:Vш2 =83дБ; - уровень вибрационного шума в 3-ей октаве:Vш3 =85дБ; - уровень вибрационного шума в 4-ой октаве:Vш4 =81дБ; - уровень вибрационного шума в 5-ой октаве:Vш5 =77дБ. Определите интегральный уровень шума в двух октавах $V_{ш4+ш5}$ [дБ]. Примечание: при необходимости выполните перевод из децибелов в м/с2 и обратно по формулам (V [м/с2] = V_0∗$10^{V\ (дБ)/20}$ (дБ)/20, где V_0=3∗10^{-4}[м/$с^2$]).	4
Решение	**<u>Вариант 1</u>:** вычисляем интегральный уровень шума $V_{ш4+ш5}$. $V_{ш4+ш5}$ = 10*lg ($10^{Vш4/10}$+$10^{Vш5/10}$) =10*lg ($10^{8.1}$+$10^{7.7}$) = 82,4554дБ. **Примечание:** в этом выражении значения $V_ш$ должны быть в децибелах. **<u>Вариант 2</u>:** вычисляем уровень шума $V_ш$: $V_{ш4+ш5} = \sqrt{V_{ш4}^2 + V_{ш5}^2}$ **Примечание:** в этом выражении значения $V_ш$ должны быть в м/$с^2$.	

	После расчета полученное значение $V_{ш4+ш5}$ переводится в децибелы. **Ответ: $L_{с45}$ = 82,46дБ.**	
11.	Для одноканальных (многоканальных) защищенных волоконно-оптических систем передачи (ВОСП) средняя мощность на входном полюсе волоконно-оптических линий передачи должна быть минимально возможной (чем меньше Р, тем выше защищенность). Известны: коэффициент дополнительных потерь в волокне $k_д = 1$ (отн. ед.); поправка для одноканальной защищенной волоконно-оптической системы передачи U, равная 0дБ и предельно допустимое изменение коэффициента передачи Ад = 0,06дБ между оптическими полюсами. Определите, чему равно относительное изменение мощности в процентах (Δотн.изм.мощн.%). Запишите ответ (в процентах) по правилу округления, до сотого знака после запятой.	5
Решение	**Δотн.изм.мощ.** = $(1 - 10^{-0,1*0,06})$ = 0,0137205 ≈ 0,0137 ; **Δотн.изм.мощн. (%)** = $(1 - 10^{-0,1*0,13})$*100 % =1,37205 ≈ 1,37%. **Проверка:** Δотн.изм.мощн. (%): 1,37% = $(1 - 10^{-0,1*А_д})$ * 100, следовательно: Δотн.изм.мощн. (%) / 100 = $(1 - 10^{-0,1*Ад}) = 0,0137 => (1 - 0,0137) = 10^{-0,1*Ад}$ => - 0,1*Ад *1 = lg (0,9863) => Ад = lg (0,9863) / (-0,1) = 0,0599 = 0,06дБ (верно). **Ответ: Δотн.изм.мощн. (%) = $(1 - 10^{-0,1*0,13})$*100 % =1,37205 ≈ 1,37%.**	
12.	Определите предельную чувствительность приемника с входным сопротивлением 50 Ом при температуре 20^0С в микровольтах, если чувствительность при полосе пропускания $\Delta f = 10$ Гц и коэффициенте различимости 3дБ составляет -142 дБм. Запишите ответ мкВ (в микровольтах) по правилу округления, до тысячного знака после запятой.	5
Решение	Находим коэффициент шума приемника $$К_ш = 174 - К_р(дБ) - 10 \cdot log(\Delta f) + Р_с, \text{ дБ}$$ или $$К_ш = 174 - 3 - 10 - 142 = 19, \text{ дБ}$$ Так как чувствительность приемника в дБ относительно микровольта равна $$U_с = К_р(дБ) - 61 + 10 \cdot log(\Delta f) + К_ш(дБ), \text{ дБмкВ}$$ $$U_с = -61 + 10 + 19 = -32, \text{ дБмкВ}$$ Тогда предельная чувствительность в микровольтах составит $$U_с = 10^{\frac{-32}{20}} = 0,025 \text{ мкВ}$$ **Ответ: $U_с$ = 0,025мкВ**	