ДОПОЛНИТЕЛЬНАЯ ОБРАЗОВАТЕЛЬНАЯ ПРОГРАММА

«Математические основы шифрования»

Структура Контрольно-Измерительного Материала (КИМ)

Настоящий КИМ используются для текущего контроля и промежуточной аттестации обучающихся по дополнительной программе «Математические основы шифрования» .

КИМ оформлены в виде тестовых заданий, охватывающие все содержание программы. Тестовые задания содержат задания с выбором ответа или группы ответов. Все тестовые задания адаптированы для электронных уроков МЭШ.

Качество выполнения каждого теста подсчитывается в процентах.

Введение в криптографию.

1. Зачем нужно изучать старые шифры?
   1) Для понимания логики развития современных алгоритмов шифрования.
   2) Для тренировки математических способностей.
   3) Для понимания современных криптографических технологий нужно знать историю создания шифров.
   4) Все выше перечисленное. (верный ответ)

2. Какой из алгоритмов шифрования относится к классическим шифрам:
   1) Алгоритм Диффи-Хелмана.
   2) Шифр Эль-Гамаля.
   3) Шифр Цезаря (верный ответ).
   4) RSA.

3. Среднестатистическая частота употребления буквы <e> в английском языке равна:
   1) 0,12702 (верный ответ)
   2) 0,09056
   3) 0,08167
   4) 0,07507
   5) 0,06966

4. Какой самый распространенный биграмм в английском языке:
   1) th (верный ответ)
   2) an
   3) er
   4) es
   5) ea
   6) at

5. Какой исторический шифр был придуман первым:
   1) шифр замены (верный ответ)
   2) шифр сдвига

3) Шифр Эль-Гамаля
4) Шифр Аристотеля

Симметричное и асимметричное шифрование.

1. Сессионный ключ:
   1) Применяется для одного сеанса связи и уничтожается в короткий промежуток времени. (верный ответ)
   2) Применяется для одного сеанса связи и уничтожается после окончания сеанса связи. (верный ответ).
   3) Назначается для старта следующего сеанса связи в момент окончания текущего сеанса связи.
   4) Сеансовый ключ необходим только для первого сеанса связи.
   5) На основе первого сессионного ключа генерируются последующие ключи.

2. Секретный (закрытый) ключ:

   используется криптографическим алгоритмом при шифровании/расшифровке сообщений и постановке цифровой подписи. (верный ответ).

   применяется для расшифровки в асимметричных криптосистемах шифрования, его компрометация не несет угрозу зашифрованному сообщению

   используется в течение долгого периода времени (от нескольких часов до нескольких лет, в зависимости от назначения). Его компрометация ставит под угрозу всю систему и является большой проблемой (верный ответ).

   применяется для различных сеансов связи и уничтожается в определенный промежуток времени по заданному алгоритму .

3. При симметричном шифровании
   1) При симметричном шифровании обе стороны используют один и тот же ключ расшифровывания (верный ответ).
   2) При симметричном шифровании обе стороны используют один и тот же алгоритм расшифровывания.
   3) При симметричном шифровании обе стороны предварительно договариваются о алгоритмах и ключе шифрования. (верный ответ).
   4) При симметричном шифровании для шифрования и расшифровывания обе стороны действуют симметрично и согласованно.

4. Можно ли расшифровать сообщение публичным (открытым) ключом?
   1) Нет. (верный ответ).
   2) Да, можно
   3) Можно при определенных условиях и методах шифрования
   4) Нет, но потеря открытого ключа может привести к компрометации шифра

5) Нет, но потеря публичного ключа может нести угрозу конкретному зашифрованному сообщению при криптоанализе.

5. PKI (Public Key Infrastructure) — это
   1) Инфраструктура открытых ключей оперирует понятием «сертификата», который содержит открытый ключ пользователя и идентифицирующую этого пользователя информацию (верный ответ).
   2) Это современная система управления криптографической защитой (верный ответ).
   3) В инфраструктур PKI входят: защищенная электронная почта, протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом IP, электронные формы и документы с электронной цифровой подписью.
   4) Инфраструктура открытых ключей, построенная на алгоритме Kerberos.