МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ «ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

Кафедра _*програмної інженерії та інформаційних технологій управління*__
(назва)

ПАКЕТ КОНТРОЛЬНИХ ЗАВДАНЬ ДЛЯ ПЕРЕВІРКИ ЗНАНЬ З ДИСЦИПЛІНИ

ОСНОВИ БЕЗПЕКИ ІС

(назва навчальної дисципліни)

рівень вищої освіти_____*перший (бакалаврський)*_____
перший (бакалаврський) / другий (магістерський)

галузь знань_____*12 Інформаційні технології*_____
(шифр і назва)

спеціальність ____*126 Інформаційні системи та технології*_____
(шифр і назва)

вид дисципліни ___*професійна підготовка*_____
(загальна підготовка / професійна підготовка)

форма навчання _____*денна*_____
(денна / заочна)

Укладач __*Євсєєв Сергій Петрович, доцент*_____
(прізвище, посада)

Харків – 2017 рік

ПОЯСНЮВАЛЬНА ЗАПИСКА

Мета контрольних завдань - перевірити ступінь сформованості у майбутніх фахівців принципів побудови комплексних систем захисту інформації, дослідження та використання сучасних процедур забезпечення надання основних послуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Контрольні завдання вимагають від студента творчого підходу, креативності, спонукають до пошукової діяльності. Вони орієнтовані на те, що слухачі повинні продемонструвати:

- Здатність застосовувати знання у практичних ситуаціях.
- Знання та розуміння предметної області та розуміння професійної діяльності.
- Здатність вчитися і оволодівати сучасними знаннями.
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки.

Перелік контрольних питань для перевірки теоретичних знань, умінь та навичок додається. Вони складені на підставі навчальної програми професійної дисципліни «ОСНОВИ БЕЗПЕКИ ІС» та робочого навчального плану підготовки фахівців освітньо-кваліфікаційного рівня „бакалавр” за сеціальністю 126 Інформаційні системи та технології у галузі знань 12 «Інформаційні технології».

Тривалість виконання контрольних завдань - 2 години

НАВЧАЛЬНА ПРОГРАМА НОРМАТИВНОЇ ДИСЦИПЛІНИ

Модуль 1. Безпека та захист даних

1. Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах та системах
2. Побудова класифікацій криптографічних засобів
3. Побудова моделі порушника безпеки в КМіС
4. Побудова моделі реалізації загроз безпеки в КМіС
5. Побудова математичної моделі пасивних атак у КМіС
6. Побудова моделі активних атак у КМіС із блокуванням передачі інформації
7. Побудова моделі активних атак у КМіС із внесенням перешкод
8. Побудова моделі активних атак "маскарад" у КМіС
9. Побудова та аналіз моделі оцінки ризику реалізації загроз безпеки комунікаційних систем
10. Оцінка ризику реалізації загроз у комунікаційних системах

Література: основна [1 – 4]; додаткова [5 – 10].

Модуль 2. Основи побудови систем захисту інформації в ПЗ

1. Використання Firewall (Брандмауер)
2. Використання Network Address Translation
3. Використання демілітаризованої зони
4. Використання другого firewall-у
5. Використання Proxy-сервер-у
6. Використання другого mail-серверу
7. Антивірусний захист поштової системи
8. Використання Log-серверу

Література: основна [1 – 4]; додаткова [5 – 10].

КРИТЕРІЇ ОЦІНЮВАННЯ ЗНАНЬ ТА ВМІНЬ СТУДЕНТІВ

Рівень досягнень/Marks				Критерії оцінювання/Evaluation criteria	
Національна оцінка National grad		Бали Local grad	Оцінка за шкалою ЄКТС ECTS grad	позитивні/pozitiv	негативні/negativ
Відмінно Excelient	5	95-100	A	Глибоке знання навчального матеріалу, що містяться в основних і додаткових літературних; Вміння аналізувати явища, які вивчаються в їхньому взаємозв'язку і розвитку; Вміння проводити теоретичні розрахунки; Відповіді на запитання чіткі, лаконічні, логічно послідовні; Вміння застосовувати теоретичні положення під час розв'язання складних практичних задач.	
Відмінно Excelient	5	90-94	B	Глибокий рівень знань в обсязі обов'язкового матеріалу, що передбачений модулем; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати складні практичні задачі.	Відповіді на запитання містять незначні неточності.
Добре Good	4	85-89	B	Глибокий рівень знань в обсязі обов'язкового матеріалу, що передбачений модулем; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати складні практичні задачі.	Відповіді на запитання містять певні неточності.
Добре Good	4	75-84	C	Міцні знання матеріалу, що вивчається, та його практичного застосування; Вміння давати аргументовані відповіді на запитання і проводити теоретичні розрахунки; Вміння вирішувати практичні задачі.	Невміння використовувати теоритичні знання для вирішення складних практичних задач.
Задовільно Satisfactory	3	65-74	D	Знання основних фундаментальних положень матеріалу, що вивчається, та їх практичного застосування; Вміння вирішувати прості практичні задачі.	Невміння давати аргументовані відповіді на запитання; Невміння аналізувати викладений матеріал і виконувати розрахунки; Невміння вирішувати складні практичні задачі.

Задовільно Satisfactory	3	60-64	E	Знання основних фундаментальних положень матеріалу модуля; Вміння вирішувати найпростіші практичні задачі.	Незнання окремих (непринципових) питань з матеріалу модуля; Невміння послідовно і аргументовано висловлювати думку; Невміння застосовувати теоретичні положення при розв'язанні практичних задач.
Незадовільно Fail	2	35-59	FX	Додаткове вивчення матеріалу модуля може бути виконане в терміни, що передбачені навчальним планом.	Незнання основних фундаментальних положень навчального матеріалу модуля; Істотні помилки у відповідях на запитання; Невміння розв'язувати прості практичні задачі.
Незадовільно Fail	2	<35	F		Повна відсутність знань значної частини навчального матеріалу модуля; Істотні помилки у відповідях на запитання; Незнання основних фундаментальних положень; Невміння орієнтуватися під час розв'язання простих практичних задач.

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 1

1. Назвіть основні послуги та механізми безпеки відповідно до стандартів ISO 7498, ISO\IES 10181.

2. Зашифруйте і розшифрувати за допомогою поліалфавітного методу шифрування відкритий текст. Відкритий текст:конфиденциальность. Ключ(и):К(2-3-4-1). Алфавіт(и):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Аоткр	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Ашифр1	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
Ашифр2	я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	е	д	г	в	б	а
Ашифр3	п	р	г	ш	к	е	й	ц	у	ъ	ф	о	л	д	ж	щ	з	х	ч	с	н	б	ю	и	э	я	т	ь	ы	в	а	м
Ашифр4	ь	к	е	д	ж	э	а	м	ъ	у	щ	з	х	ф	о	л	б	п	р	г	ш	ю	й	ц	и	ч	с	н	я	т	ы	в

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення конфіденційності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 12 ПК (у першому – 8 комп'ютерів, у другому – 4), які об'єднані в автономні локальні мережі за технологіями Token Ring і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT другої форми, proxy-сервера та шлюзу прикладного рівня з брандмауером.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "A".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Расшифруйте повідомлення M, яке отримано від користувача "F".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	F	A	67	--	--

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор

доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 2

1. Назвіть основні механізми забезпечення автентичності повідомлень.
2. Зашифруйте і розшифрувати за допомогою шифру Цезаря з ключовим словом відкритий текст. *Відкритий текст:*автентичність. *Ключ(и):* шифр. *Алфавіт(и): український*
3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму асиметричного шифрування для забезпечення конфіденційності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами на основі хешування.
4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 18 ПК (у першому – 8 комп'ютерів, у другому – 10), які об'єднані в автономні локальні мережі за технологіями FDDI і Fast Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 3 форми, демілітаризованої зони з необхідними серверами.
5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "B".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Расшифруйте повідомлення M, яке отримано від користувача "C".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	C	B	88	--	--

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 3

1. Назвіть основні механізми забезпечення цілісності.

2. Зашифруйте і розшифрувати за допомогою поліалфавітного методу шифрування відкритий текст. Відкритий текст: целостность. Ключ(и):К(4-3-1-2). Алфавіт(и):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Аоткр	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Ашифр1	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
Ашифр2	я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	е	д	г	в	б	а
Ашифр3	п	р	г	ш	к	е	й	ц	у	ъ	ф	о	л	д	ж	щ	з	х	ч	с	н	б	ю	и	э	я	т	ь	ы	в	а	м
Ашифр4	ь	к	е	д	ж	э	а	м	ъ	у	щ	з	х	ф	о	л	б	п	р	г	ш	ю	й	ц	и	ч	с	н	я	т	ы	в

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення автентичності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 10 ПК (у першому – 4 комп'ютера, у другому – 6), які об'єднані в автономні локальні мережі за технологіями Fast Ethernet і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 1 форми, proxy-сервера та шлюзу прикладного рівня з брандмауером.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "C".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Расшифруйте повідомлення M, яке отримано від користувача "F".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значенння	ЦП
Шифрування RSA	F	C	156	--	--

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 4

1. Назвіть основні механізми забезпечення управління доступом.
2. Зашифруйте і розшифрувати за допомогою шифру простої заміни відкритий текст. *Відкритий текст:*політика безпеки. *Ключ(и):* задати самостійно. *Алфавіт(и):український*
3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму асиметричного шифрування для забезпечення конфіденційності та автентичності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами хешування.
4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 13 ПК (у першому – 8 комп'ютерів, у другому – 5), які об'єднані в автономні локальні мережі за технологіями Token Ring і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 3 форми, proxy-сервера та Log-Сервера.
5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "D".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Расшифруйте повідомлення М, яке отримано від користувача "А".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	A	D	164	--	--

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 5

1. Назвіть основні механізми забезпечення приналежності.
2. Зашифруйте і розшифрувати за допомогою шифру Цезаря відкритий текст. *Відкритий текст:*захист інформації. *Ключ(и):*визначити самостійно. *Алфавіт(и):український*
3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму асиметричного шифрування для забезпечення ЦП на основі RSA. Визначити достоїнства та недоліки даного протоколу.
4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 20 ПК (у першому – 13 комп'ютерів, у другому – 7), які об'єднані в автономні локальні мережі за технологіями Token Ring і FDDI відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 3 форми, демілітаризованої зони з необхідними серверами.
5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "F".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Расшифруйте повідомлення M, яке отримано від користувача "E".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	E	F	127	--	--

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 6

1. Назвіть які рівні EMBBC відповідають за основні послуги та механізми безпеки відповідно до стандартів ISO 7498, ISO\IES 10181.

2. Зашифруйте і розшифрувати за допомогою матричного методу шифрування відкритий текст. *Відкритий текст:*стеганографія. *Ключ(и):*$К_1$(2-3-4-1-5). $К_1$(2-4-5-1-3).

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму МАС-коду для забезпечення конфіденційності та автентичності. Визначити достоїнства та недоліки даного протоколу.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 15 ПК (у першому – 7 комп'ютерів, у другому – 8), які об'єднані в автономні локальні мережі за технологіями Fast Ethernet і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT другої форми, proxy-сервера та Log-Сервера.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "D".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Перевірте цифровий підпис повідомлення M, отриманого від користувача "E"

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	E	D	164	45	66

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"

Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 7

1. Які елементи повинна включати в себе політика безпеки.

2. Зашифруйте і розшифрувати за допомогою поліалфавітного методу шифрування відкритий текст. Відкритий текст:асимметричное шифрование. Ключ(и):К(2-4-1-3). Алфавіт(и):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Аоткр	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Ашифр1	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
Ашифр2	я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	е	д	г	в	б	а
Ашифр3	п	р	г	ш	к	е	й	ц	у	ъ	ф	о	л	д	ж	щ	з	х	ч	с	н	б	ю	и	э	я	т	ь	ы	в	а	м
Ашифр4	ь	к	е	д	ж	э	а	м	ъ	у	щ	з	х	ф	о	л	б	п	р	г	ш	ю	й	ц	и	ч	с	н	я	т	ы	в

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення ЦП та автентичності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 14 ПК (у першому – 6 комп'ютерів, у другому – 8), які об'єднані в автономні локальні мережі за технологіями Token Ring і Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 1 форми, proxy-сервера та шлюзу прикладного рівня з брандмауером.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "E".

Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.

Перевірте цифровий підпис повідомлення M, отриманого від користувача "A"

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	A	E	24	35	48

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 8

1. Назвіть основні принципи інформаційних відносин відповідно до Закону України "Об інформації"

2. Зашифруйте і розшифрувати за допомогою методу шифрування простої заміни відкритий текст. *Відкритий текст:*управління доступом. *Ключ(и):*визначити самостійно.

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення конфіденційності, ЦП та автентичності. Визначити достоїнства та недоліки даного протоколу.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 16 ПК (у першому – 10 комп'ютерів, у другому – 6), які об'єднані в автономні локальні мережі за технологіями FDDI і Fast Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою NAT 3 форми, proxy-сервера.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "D".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Перевірте цифровий підпис повідомлення M, отриманого від користувача "B"

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	B	D	151	49	275

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"
Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 9

1. Які види інформації визначені у Законі України "Об інформації".

2. Зашифруйте і розшифрувати за допомогою шифру Цезаря ключем відкритий текст. *Відкритий текст:* віра та любов. *Ключ(и):рулетка*. *Алфавіт(и):український*

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму симетричного шифрування для забезпечення конфіденційності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 14 ПК (у першому – 8 комп'ютерів, у другому – 6), які об'єднані в автономні локальні мережі за технологіями FDDI і Fast Ethernet відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою proxy-сервера та шлюзу прикладного рівня з брандмауером.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "C".
Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.
Перевірте цифровий підпис повідомлення M, отриманого від користувача "D"

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	D	C	231	76	119

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор
доцент С.П. ЄВСЕЄВ

Національний технічний університет «Харківський політехнічний інститут»
Кафедра програмої інженерії та інформаційних технологій управління

Дисципліна "Технології захисту інформації"

Спеціальність «Комп'терні науки», «Інженерія програмного забезпечення»

Білет № 10

1. Що розуміється під політикою безопасноті.

2. Зашифруйте і розшифрувати за допомогою поліалфавітного методу шифрування відкритий текст. Відкритий текст:украинский язык. Ключ(и):К(1-4-2-3). Алфавіт(и):

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Аоткр	а	б	в	г	д	е	ж	з	и	й	к	л	м	н	о	п	р	с	т	у	ф	х	ц	ч	ш	щ	ъ	ы	ь	э	ю	я
Ашифр1	й	ц	у	к	е	н	г	ш	щ	з	х	ъ	ф	ы	в	а	п	р	о	л	д	ж	э	я	ч	с	м	и	т	ь	б	ю
Ашифр2	я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	е	д	г	в	б	а
Ашифр3	п	р	г	ш	к	е	й	ц	у	ъ	ф	о	л	д	ж	щ	з	х	ч	с	н	б	ю	и	э	я	т	ь	ы	в	а	м
Ашифр4	ь	к	е	д	ж	э	а	м	ъ	у	щ	з	х	ф	о	л	б	п	р	г	ш	ю	й	ц	и	ч	с	н	я	т	ы	в

3. Побудуйте протокол обміну інформації між користувачами А і В за допомогою алгоритму хешування для забезпечення конфіденційності, ЦП та автентичності. Визначити достоїнства та недоліки даного протоколу. Порівняйте з протоколами асиметричного шифрування.

4. У корпоративній мережі компанії, що розташовується в 2-х будинках (4 поверхи та 2 поверхи відповідно), розміщені рівномірно 17 ПК (у першому – 8 комп'ютерів, у другому – 9), які об'єднані в автономні локальні мережі за технологіями Token Ring і FDDI відповідно. Розробити структурну схему захисту корпоративної мереж компанії, обґрунтувати та запропонувати необхідні протоколи і програмно-апаратні засоби для забезпечення конфіденційного обміну інформацією між користувачами другого будинку; забезпечити надійний захист при виході користувачів до мережі Internet за допомогою демілітаризованої зони з необхідними серверами.

5. Ви є користувачем розподіленої захищеної системи з 6 користувачами. У даній системі користувачі можуть здійснювати асиметричне зашифрування (расшифрування) RSA і виробляти або перевіряти цифровий підпис на основі RSA для повідомлень.

Користувачі системи

Користувач	Параметр системи n		Ключі користувачів	
	p	q	Особливий (секретний) d	Відкритий (публічний) e
A	11	23	19	
B	17	19		137
C	11	17	37	
D	13	19		67
E	17	23	111	
F	13	17		97

Ви користувач "F".

Перевірити, що ваші ключі (відкритий і особливий) відібрані правильно.

Перевірте цифровий підпис повідомлення M, отриманого від користувача "A".

Формат повідомлення

Тип алгоритму	Відправник	Отримувач	Повідомлення	Хеш-значеннння	ЦП
Шифрування RSA	A	F	321	65	82

Затверджено на засіданні кафедри інформаційних систем протокол № 09 від 20.02.2016 р.

Завідувач кафедри
професор М.Д. ГОДЛЕВСЬКИЙ

Екзаменатор

доцент С.П. ЄВСЕЄВ

НАВЧАЛЬНО-МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Євсеєв С.П. Лабораторний практикум з дисципліни “Технології захисту інформації” [Електронний ресурс]. – Режим доступу: ntumoodle.com

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова

1. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

2. Кузнецов О. О. Захист інформації в інформаційних систе-мах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

3. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом “Родовід”, 2014. – 428 с.

4. Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Допоміжна література

5. Ленков С.В. Методы и средства защиты информации. В 2-х томах/ С. В. Ленков, Д. А. Перегудов, В. А. Хорошко.– К.: Арий, 2008. – Т.II. Информационная безопасность. – 344 с.

6. Мао Венбо Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом “Вильямс”, 2005. – 768 с.

7. Петров А.А. Компьютерная безопасность. Криптографические методы защиты. / А. А. Петров– М.: ДМК, 2000. – 448 с.

8. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.1. – 292 с.

9. Поповский В.В. Защита информации в телекоммуникационных системах: Учебник: В 2 т. / В. В. Поповский, А. В. Персиков. – Харьков: ООО “Компания СМИТ”, 2006. – Т.2. – 252 с.

10. Чмора А.Л. Современная прикладная криптография. / А. Л. Чмора. – М.: Гелиос АРВ, 2001. – 256 с.

ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ

11. http://bezopasnost.biz.

12. http://dstszi.gov.ua.
13. http:// securitylab.ru
14. http:// pgpi.org
15. http:// citmgu.ru