

СОФИЙСКИ УНИВЕРСИТЕТ "СВ. КЛИМЕНТ ОХРИДСКИ"
ФАКУЛТЕТ ПО МАТЕМАТИКА И ИНФОРМАТИКА

Приет на заседание на катедра "Изчислителни системи"
с протокол № .../..... година

Утвърдил:

Декан:

проф. дмн И. Сосков

1. ОБЩО ПРЕДСТАВЯНЕ НА ДИСЦИПЛИНАТА
наименование на дисциплината: Криптография
лектор: проф. дмн Иван Ланджев, д-р Юри Борисов,

кредити	общ хорариум	часове седмично	уч. година, семестър	форма на обучение	специал- ност	статут на дисципли- ната
	60	3+1+0	летен	редовно	"	избираема

2. УЧЕБНИ ФОРМИ

Аудиторни	часове	извънаудиторни	часове
Лекции	45	курсова работа	
семинарни занятия (упражнения)	15	контролна работа	

3. ФОРМИРАНЕ НА ОЦЕНКАТА ПО ДИСЦИПЛИНАТА

	% от оценката
Текуща оценка	
– курсова работа	
– котролна работа	
– активно учатие в часовете	
– присъствие в час	
Изпит	100 %
– практически (задачи)	- 25 %
– теоретичен	- 75%

4. ПРИЛОЖЕНИЯ

Приложение 1: Анотация на дисциплината

Приложение 2: Тематичен план на дисциплината по учебни часове

Приложение 3: Конспект за изпит

Приложение 4: Библиография за курса и изпита

АНОТАЦИЯ

Курсът „Криптография“ предполага познания по дискретна математика и алгебра в рамките на стандартните университетски курсове, както и по елементарна теория на числата. Материалът е организиран така, че да следва историческото развитие на дисциплината. В началото се излагат някои класически криptosистеми, които водят до важни теоретични обобщения. По-нататък се излага понятието свършена секретност, следвайки теоретико-информационния подход на Шенон. Специално внимание се отделя на двете големи групи симетрични шифри, т.нар. поточни и блокови шифри. Отделна лекция е посветена на новия стандарт за блоков шифър Rijndael. Обсъждат се линейният и диференциалният анализ на блокови шифри, както и устойчивостта на Rijndael към тези атаки. В частта на курса, посветена на асиметричната криптография, се обсъждат най-вече алгоритмичните страни на теоретико-числовите задачи, които водят до най-популярните криptosистеми – задачата за разлагане на прости множители и задачата за намиране на дискретен логаритъм в мултипликативната група на крайно поле. Наред с широко известните криптографски системи RSA, DSA, MacEliece, се разглеждат и някои компрометирани криptosистеми (Merkle-Hellman), представляващи теоретичен интерес. Внимание е отделено на някои специални криптографски протоколи – удостоверяване на самоличност, електронен кеш, електронно гласуване, генериране на случаен бит и др., както и на някои схеми за разпределение на данни.

ТЕМАТИЧЕН ПЛАН

№	ТЕМА	лекции	упражнения
1	Класическа криптография	2	
2	Теория на Шенон	1	
3	Поточни шифри	2	
4	Блокови шифри	2	
5	Асиметрични шифри	7	
6	Криптографски протоколи		

КОНСПЕКТ

1. Исторически преглед на класическата криптография (проста субституция, шифър на Vigenere, шифър на Playfair, транспозиционни шифри, шифър на L. Hill, ENIGMA, M-209). Криптоанализ.
2. Приложение на Булевите функции в криптографията
3. Съвършена секретност (теория на Shannon).
4. Линейни рекурентни редици. Постулати на Golomb. Поточни шифри.
5. Алгоритъм на Berlekamp-Massey.
6. Блокови шифри (DES, IDEA, Rijndael, RC6).
7. Диференциален и линеен криптоанализ на блокови шифри.
8. Асиметрична криптография (общи сведения).
9. RSA (генериране на големи прости числа, задача за разлагане на прости делители).
10. Задача за намиране на дискретен логаритъм. Цифров подпис (Diffie-Hellman, El Gamal, DSA).
11. Алгоритъм на Pohlig-Hellman за намиране на дискретен логаритъм.
12. Задача за раницата. Криптосистема на Merkle-Hellman. Криптанализ на Шамир.
13. Криптосистеми, базирани на елиптични криви.
14. Генериране на случаен бит.
15. Схеми за разпределяне на данни (secret sharing schemes).
16. Някои криптографски протоколи.

БИБЛИОГРАФИЯ

1. Ланджев, И. , *Записки по криптография*, 2005.
2. Koblitz, N. , *A Course in Number Theory and Cryptography*, Springer-Verlag, 1998.
3. Menezes, A. , P. van Oorschot, S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.
4. Salomaa, A. , *Public-Key Cryptography*, Berlin, Springer-Verlag, 1990.
5. Strinson, D. R., *Cryptography: Theory and Practice*, CRC, Boca Raton-London-Tokyo, 1995.
6. Van Tilborg, H. C.A., *An Introduction to Cryptology*, Kluwer Academic Publishers, 1988.
7. Beker, H., F. Piper, *Cipher systems: the protection of communications*, London, Northwood Books, 1982.