

æ

UYGULAMALI MATEMATİK ENSTİTÜSÜ, Kriptografi Bölümü
ODTÜ, TÜRKİYE



KRİPTOLOJİYE GİRİŞ DERS NOTLARI

UYGULAMALI MATEMATİK ENSTİTÜSÜ

Kriptolojiye Giriş Ders Notları,

Prof. Dr. Ersan Akyıldız

Doç. Dr. Ali Doğanaksoy

Yrd. Doç. Ebru Keyman

Dr. Muhiddin Uğuz

gözetimi altında aşağıda adı geçen kişiler tarafından hazırlanmıştır:

Kadir Altan

Kerem Kaşkaloglu

Nihal Kındap

Çiğdem Özakın

Zülfükar Saygı

Elif Yıldırım

Murat Yıldırım

Senay Yıldız

Derleyenler: Ebru Keyman - Murat Yıldırım

İÇİNDEKİLER

1	GİRİŞ	1
2	BLOK ŞİFRELER	3
2.1	Blok Şifre Sistemlerinin Parametreleri	7
2.1.1	Blok Uzunluğu	7
2.1.2	Anahtar ve Gerçek Anahtar Uzunluğu	7
2.2	Blok Şifre Sistemlerinin Tasarım Ölçütleri	8
2.2.1	Yayılma	8
2.2.2	Nüfuz Etme	9
2.3	Döngülü (Iterated) Blok Şifre Sistemleri	9
2.4	Feistel Yapılar	10
3	DES	11
3.1	DES Algoritması	11
3.1.1	Başlangıç Permütasyonu	12
3.1.2	Başlangıç Permütasyonunun Tersisi	12
3.1.3	Anahtar Permütasyonu ve Döngü Anahtarının Üretilmesi	13
3.1.4	f fonksiyonu	14
3.2	DES'in Tasarım Özellikleri	17
4	RIJNDAEL	19

UYGULAMALI MATEMATİK ENSTİTÜSÜ

4.1	Matematiksel Özellikler	19
4.1.1	Toplama İşlemi	19
4.1.2	Çarpma İşlemi	20
4.2	Algoritma	24
4.2.1	Byte Sub	25
4.2.2	Shift Row	26
4.2.3	Mix Column	26
4.2.4	Anahtarla XOR'lama	27
4.3	Anahtar Algoritması	28
4.4	ALGORİTMANIN TERSİ	31
4.4.1	Mix Column	31
4.4.2	Byte Sub	31
5	AKAN ŞİFRELER.....	32
5.1	One Time Pad Sistemi	33
5.1.1	Sistemin Avantajları	33
5.1.2	Sistemin Dezavantajları	33
5.2	Dizi Üreticiler	34
5.3	Geri Beslemeli KaydırmalıYazdırgaç (Feedback Shift Register)	37
5.4	Üreticinin Sahip Olması Gereken Özellikler	41
5.4.1	İstatistiksel Özellikler	41
5.5	Doğrusal Geri Beslemeli KaydırmalıYazdırgaç (LFSR)	44
5.5.1	Dizinin Periyodu	47
5.6	Doğrusal Karmaşıklık (Linear Complexity)	49

UYGULAMALI MATEMATİK ENSTİTÜSÜ

5.6.1	Doğrusal Karmaşıklık Profili (Linear Complexity Profile)	50
5.6.2	Berleekamp Massey Algoritması	51
5.7	LFSR Kullanılarak Yapılan Akan Şifre Sistemleri	52
6	SAYILAR TEORİSİ	58
6.1	Tamsayılar	58
6.1.1	Bölünebilirlik:	58
6.1.2	Bölünebilirlik Özellikleri	58
6.1.3	Tamsayılar için Bölüm Algoritması:	59
6.1.4	En Büyük Ortak Bölen (Greatest Common Divisor)	59
6.1.5	En Küçük Ortak Kat (Least common Multiple)	60
6.1.6	Asal Sayı	60
6.1.7	Aralarında Asal Sayı	61
6.1.8	Aritmetiğin Esas Teoremi	61
6.1.9	Öklid Algoritması(Euclidean Algorithm)	61
6.2	Asal Sayılar	64
6.2.1	Eratosthenes Kalburu(The Sieve of Eratosthenes)	64
6.3	Eratosthenes Metodu (Method of Eratosthenes)	65
6.4	Denklik Teorisi(Theory of Congruence (Modularity))	66
6.4.1	Teoremler:	66
6.4.2	Aritmetik Tersisi	67
6.5	Euler $\Phi(\phi)$ Fonksiyonu (Euler Phi Function)	68
7	AÇIK ANAHTARLI SİSTEMLER	70

UYGULAMALI MATEMATİK ENSTİTÜSÜ

7.1	MERKLE-HELLMAN KNAPSACK KRIPTOSİSTEM	70
7.1.1	Süperartan dizi (Superincreasing sequence)	71
7.1.2	Süperartan Altküme Toplama Problemini çözme Algoritması	71
7.1.3	Merkle-HellmanKnapsack Şifrelemesinde Anahtar Oluşturma Algoritması	72
7.1.4	Basit Merkle-Hellman Knapsack Açık Anahtar Şifreleme Algoritması	73
7.2	RSA Kriptosistem	75
7.3	RSA İmza Şeması	79
7.3.1	İmzalama	79
7.3.2	İmzayı Doğrulama	80
7.4	Ayrık Logaritma(Discrete Logarithm)	81
7.5	El-Gamal Açık Anahtarlı Kriptosistem	81
7.6	ElGamal Açık Anahtarlı Şifrelemede Anahtar Oluşturma Algoritması	82
7.6.1	ElGamal Açık Anahtarlı Şifreleme Algoritması	82
7.6.2	ElGamal İmzası	84
7.6.3	İmza Algoritması	84
7.6.4	Doğrulama	84
7.7	Diffie-Hellman Anahtar Anlaşması (Diffie-Hellman Key Agreement)	86
7.7.1	Diffie-Hellman Anahtar Anlaşması Algoritması:	86
8	KRİPTANALİZ	88
8.1	Kriptanalitik Atakların Amaçları	90
8.2	Kriptanaliz Metodları(Methods of Cryptanalysis)	91

UYGULAMALI MATEMATİK ENSTİTÜSÜ

8.3	Akan Şifrelerin Analizi	93
8.4	Blok Şifrelerin Analizi	97
8.4.1	Difransiyel Kriptanaliz	97
8.4.2	Doğrusal Kriptanaliz	105
9	HASH FONKSİYONLARI.....	108
10	TEST YÖNTEMLERİ.....	115
11	KRİPTOGRAFİK PROTOKOLLER.....	123