Gün	Tarih	Sunum Saati	Proje Konusu
1. Gün	27.11.2026	14.00 – 14.10	Blowfish
1. Gün	27.11.2026	14.10 – 14.20	Skipjack
1. Gün	27.11.2026	14.20 – 14.30	Serpent
1. Gün	27.11.2026	14.30 – 14.40	RC6
1. Gün	27.11.2026	14.40 – 14.50	IDEA
1. Gün	27.11.2026	14.50 – 15.00	Camellia
2. Gün	04.12.2026	14.00 – 14.10	Cramer-Shoup
2. Gün	04.12.2026	14.10 – 14.20	Elliptic Curve DSA (ECDSA)
2. Gün	04.12.2026	14.20 – 14.30	Boneh–Lynn–Shacham (BLS)
2. Gün	04.12.2026	14.30 – 14.40	GOST R 34.10
2. Gün	04.12.2026	14.40 – 14.50	Paillier
2. Gün	04.12.2026	14.50 – 15.00	Rabin
3. Gün	11.12.2026	14.00 – 14.10	ML-KEM (CRYSTALS-Kyber) – 1
3. Gün	11.12.2026	14.10 – 14.20	ML-KEM (CRYSTALS-Kyber) – 2
3. Gün	11.12.2026	14.20 – 14.30	ML-KEM (CRYSTALS-Kyber) – 3
3. Gün	11.12.2026	14.30 – 14.40	ML-DSA (CRYSTALS-Dilithium) – 1
3. Gün	11.12.2026	14.40 – 14.50	ML-DSA (CRYSTALS-Dilithium) – 2
3. Gün	11.12.2026	14.50 – 15.00	SLH-DSA (SPHINCS+) – 1
3. Gün	11.12.2026	15.00 – 15.10	SLH-DSA (SPHINCS+) – 2

Değerlendirme Kriterleri:

1-) Algoritmalar özelliğine göre aşama aşama (algoritma türüne göre geçirdiği tüm ara aşamalar istenildiğinde konsolda görülebilecektir) sonuçlar gösterilerek istenilen herhangi bir programlama dilinde kodlanabilir. Ancak hazır kütüphanelerle değil, kodları kendiniz yazmanız gerekmektedir.

2-) İstenilen Plaintext (yazı, dosya yada görüntü) üzerinde şifreleme yapılabilmesi gerekir. (Her veri türünde şifrelemeye uygun olmayan algoritmaların neden yapamadığı açıklanmalıdır.)

3-) Proje sunumları belirtilen saatlerde 103 No'lu derslikte yapılacaktır. (Belirtilen gün ve saatte yapılmayan sunumlar geçersiz sayılacaktır.) Sunumlar geliştirilen algoritma üzerinden

öğrenci bilgisayarında yapılacaktır. Ayrıca Powerpoint tarzı sunum hazırlamaya gerek yoktur ancak gerekiyorsa algoritmayı anlatmak için farklı materyallerden faydalanılabilir.

4-) Proje sunumuyla birlikte ortalama 5 sayfalık rapor algoritmayı ve yapılan uygulamayı detaylı şekilde anlatan bir doküman çıktı alınarak ve dijital ortamda getirilmelidir. Proje dokümanı da değerlendirmenin bir parçası olacaktır.

5-) Her öğrenci hazırladığı dokümanla birlikte yazdığı kodları (kodlar txt olarak) da dijital olarak RAR uzantılı tek bir dosya halinde (dosya adı öğrenci no ve öğrenci adı soyadı olacak şekilde örnek dosya adı 220951699_tahaetem.rar) sunum günü flash veya mail ile iletecektir. Dokümanların veya kodların birbirine ve dış kaynaklara olan benzerliği de değerlendirme kriteri olarak kullanılacaktır.

6-) Her öğrenci listede belirtilen algoritma üzerinde çalışmalıdır. Farklı algoritmalar kabul edilmeyecektir. Algoritma ismine göre araştırma yapıp çalışma sistemini öğrenmek öğrenci sorumluluğundadır.

ÇANKIRI KARATEKİN ÜNİVERSİTESİ

2026-2027 Yılı Güz Dönemi – Proje Listesi

Ders Kodu ve Adı : BİL432.1.1 - Kriptografi ve Bilgi Güvenliği

Öğretim Elemanı : Doç. Dr. Taha ETEM

MÜHENDİSLİK FAKÜLTESİ / / Bilgisayar Mühendisliği

No	Öğrenci No	Adı	Soyadı	Proje konusu
1	210905014	Süleyman	Miçooğulları	Blowfish
2	220905004	Muhammed Yusuf	Ihlamur	SkipJack
3	220905081	Yusuf	Çifçi	Serpent

4	230905002	Yasin	Uğur	RC6
5	230905011	Beyza Nur	Karayel	IDEA
6	230905012	Büşra	Aydoğmuş	Camelia
7	230905013	Burak	Altundaş	Cramer-Shoup
8	230905016	Burak	Oktay	Eliptic Curve DSA
9	230905018	Rüveyda Özge	Selçuk	Boneh–Lynn–Shacham
10	230905020	Emine Zeynep	Öztürk	GOST R 34.10
11	230905026	Bayram	Sanat	Paillier
12	230905031	Tuğba Nur	Gülüç	Rabin
13	230905033	Hüseyin	Aksal	ML-KEM (CRYSTALS-Kyber)-1
14	230905034	Berkant	Özkan	ML-KEM (CRYSTALS-Kyber)-2
15	230905041	Alperen	Demirbaş	ML-KEM (CRYSTALS-Kyber)-3
16	230905051	Sibel	Yıldırım	ML-DSA (CRYSTALS-Dilithium)-1
17	230905066	Betül	Baylan	ML-DSA (CRYSTALS-Dilithium)-2
18	230905069	Betül Zülal	Kekillioğlu	SLH-DSA (SPHINCS+)-1
19	230905074	Ömer	Güler	SLH-DSA (SPHINCS+)-2