ÖDEV

DERSİN ADI : KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ
DERSİN KODU : BİL 470
DERSİN SAAT VE KREDİSİ : (3+0=3)
TESLİM TARİHİ : 30.12.2022 17:30)

Araştırma: • Hafif siklet(lightweight) simetrik şifreleme algoritmaları ve yeni önerilen algotirmaların analizi ve karşılaştırmalı olarak açıklayın. (BIL470-liste-konu, Verilen listede belirtilen iki adet kriptogtrafi algoritması için). https://csrc.nist.gov/Projects/lightweight-cryptography/email-list ve Lightweight Cryptography | CSRC (nist.gov) bu bağlantıdaki bilgiler kullanılacak

.

Programlama projesi: : C veya phyton ile gerçekleştirilecek olan bu araçta şifreleme/deşifreleme ve Özüt alma, dosya bütünlüğünün denetimi yöntemleri bizzat gerçeklenecek olup, arşiv/API kullanılmayacaktır. Gerçeklenenen Programların kaynak kodları açıklamalı olarak verilecektir;

a) İncelenen iki adet hafif siklet şifreleme algoritmalarının gerçeklenmesi ve şifreleme/ deşifrelemede kullanılması(test verileri ile birlikte).
b) Gerçeklenen Şimetrik şifreleme algoritması kullanılarak CBC ve OFB modlarında çalışmayı gerçekleyip testlerini yapacak şekle getiriniz.
c) Herhangi bir doküman (.doc/.docx, .pdf, ppt, xls vs) üzerinde değişiklik yapılıp yapılmadığını ve yapanın kimliğini anlamak için, özütünü alacak ve sadece işlem yapan kişinin bildiği bir anahtar ile şifreleyip dosyanın sonuna ekleyecek bir araç (b şıkkındaki gerçeklemeyi özüt fonk. Olarak kullanınız)
d) Dosyanın bütünlüğünün değişip değişmediğinin kontrolü için, c)deki işlemleri yaparak ilk üretilen özüt değer ile karşılaştıran doğrulama aracını gerçekleyerek örnek testleri gösteriniz.

.

Ödev problemlerinde yapılan çalışma sonuçları yazılı rapor halinde .doc/docx olarak verilen bitirme zamanından önce teams'deki ders grubuna yüklenecektir.

Başarılar. Dilerim.

ALGORİTMALAR

#	Öğrenci No	Adı Soyadı	Alg1	Alg2
1	131044075	MUHAMMET MELİH KAVRAZ	GIFT-COFB	Xoodyak
2	151044045	MEVLÜT REHA İNAN	GIFT-COFB	Photon-Beetle,
3	161044010	ÖMER FARUK BİTİKÇİOĞLU	ISAP,	Xoodyak
4	161044019	İRFAN KARATEKİN	Elephant,	Photon-Beetle,
5	161044047	SALİHA DERİN	Photon-Beetle	Sparkle,
6	171044002	ABDULLAH ÇELİK	Grain128-AEA	ISAP,
7	171044015	BERKCAN EKİCİ	ASCON	Photon-Beetle,
8	171044024	NEVZAT SEFEROĞLU	ISAP,	Sparkle,
9	171044034	MUSTAFA GÜRLER	ISAP,	Photon-Beetle,
10	171044041	BERK PEKGÖZ	ASCON	Grain128-AEAD
11	171044047	ASLI BAYRAM	Grain128-AEA	TinyJambu
12	171044048	MUHAMMED GEÇGELOĞLU	GIFT-COFB	Sparkle,
13	171044061	AYŞE DEĞİRMENCİ	ASCON	Elephant,
14	171044063	ERDİ BAYIR	ASCON	TinyJambu
15	171044071	SALİH TANGEL	Photon-Beetle	Romulus,
16	171044073	BERKAN AKIN	ASCON	ISAP,
17	171044074	KIVANÇ TÜRKER	Elephant,	Romulus,
18	171044076	ŞEYMA NUR CANBAZ	Sparkle,	Xoodyak
19	1801042086	OĞUZHAN ERDEM TEKEL	ISAP,	TinyJambu
20	1801042091	SİNAN SARI	Romulus,	Xoodyak
21	1801042092	MELİHCAN ÇİLEK	Elephant,	Xoodyak
22	1801042093	MUSTAFA HALİL ŞENOL	ISAP,	Romulus,
23	1801042097	UMUT AY ALPER	TinyJambu	Xoodyak
24	1801042102	SEDEF ERDOĞDU	Photon-Beetle	Xoodyak
25	1801042607	MUHAMMED İKBAL YAZICI	GIFT-COFB	TinyJambu
26	1801042609	YAKUP TALHA YOLCU	TinyJambu	Romulus,
27	1801042611	HATİCE SEVRA GENÇ	Elephant,	ISAP,
28	1801042614	SAMET NALBANT	Photon-Beetle	TinyJambu
29	1801042630	MEHMET AVNİ ÇELİK	Elephant,	Sparkle,
30	1801042635	YUNUS EMRE GEYİK	Sparkle,	Xoodyak
31	1801042639	AHMET YAZICI	Grain128-AEA	Sparkle,
32	1801042646	ERKUT DERE	ASCON	Xoodyak
33	1801042651	MERVE HORUZ	GIFT-COFB	ISAP,
34	1801042656	SÜLEYMAN GÖLBOL	Sparkle,	TinyJambu
35	1801042659	YUNUS EMRE YUMŞAK	Photon-Beetle	ISAP,
36	1801042668	ATAKAN ALTIN	Grain128-AEA	Xoodyak
37	1801042672	SERDİL ANIL ÜNLÜ	Romulus,	TinyJambu
38	1801042691	HACER DURSUN	Elephant,	Grain128-AEAD
39	1901042252	BARIŞ AYYILDIZ	ASCON	GIFT-COFB
40	1901042258	ABDURRAHMAN BULUT	Grain128-AEA	Photon-Beetle,
41	1901042260	BURAK ÇİÇEK	ASCON	Romulus,
42	1901042631	GÖKBEY GAZİ KESKİN	Elephant,	GIFT-COFB
43	1901042667	BURCU SULTAN ORHAN	ASCON	Sparkle,
44	1901042680	SENA ERDOĞAN	Romulus,	Sparkle,
45	1901042685	MERVE GÜRLER	GIFT-COFB	Grain128-AEAD
46	1901042692	AHMET TUĞKAN AYHAN	Grain128-AEA	Romulus,
47	1901042695	YUSUF TALHA ALTUN	ISAP,	Grain128-AEAD
48	1901042697	MUHAMMED BEDİR ULUÇAY	GIFT-COFB	Romulus,
49	200104004095	MEHMET HÜSEYİN YILDIZ	Elephant,	TinyJambu