**KRİPTOGRAFİ VE BİLGİSAYAR GÜVENLİĞİ**

**BİL 470**

**MİDTERM PROJE RAPORU**

**Muhammed Mücahit ÜÇER**

**161044030**

**UYGULAMA KATMANI**

PGP

Pretty Good Privacy,internet veri aktarımı için kriptografik gizlilik ve kimlik doğrulama sunan bir veri şifreleme ve şifre çözme bilgisayar programıdır.

**Avantajları**

-algoritması güçlüdür, kırılmaz. bir bilgisayar korsanının, devletlerin veya devlet kurumlarının PGP şifrelemesiyle korunan dosyalara veya e-postalara girmesi imkansızdır.

**Dezavantajları**

**-Complexity of use:** Verileri ve dosyaları PGP kullanarak şifrelemek zaman ve çaba gerektirir, bu da kullanıcılar için mesaj göndermeyi zorlaştırabilir.

**-Key management:** PGP’nin yanlış kullanımı sonucunda anahtar bozulabilir.

**-Lack of anonymity:** Kullanıcılara anonimlik sağlamaz.

**-Compability:** farklı versiyon programlarda çalışmaz.

S / MIME

S/MIME, Multipurpose Internet Mail Extension’un güvenliği geliştirilmiş sürümüdür.

e-postaları şifrelemek, deşifrelemek ve imzalamak için açık anahtarlı kriptografi kullanılır.

PGP S/MIME

1. sadece düz text için tasarlanmıştır multimedia dosyalar için de kullanılır

2. düşük maliyet yüksek maliyet

3. kişisel kullanım için uygundur endüstriyel kullanıma uygundur

4. 4096 public keys içerir. sadece 1024 public keys.

5. VPN’ler içinde kullanılır sadece e-posta servisleri kullanır

6. Diffie hellman digital imzayı kullanır Elgamal digital imzayı kullanır

**TAŞIMA KATMANI**

TLS

**Advantajları**

***-* Prevents tampering and eavesdropping:** TLS şifrelemesi, kötü niyetli kişilerin web tarayıcısı ve istemci arasına girmesini engeller

**-data integrity:** TLS'yi uygulamak, güvenli bir ortam üzerinden iletilen tüm verilerin herhangi bir kayıp olmaksızın hedefine ulaşmasını sağlar.

**- Trustworthy:** TLS ile güvence altına alınan siteler, müşterilerinize güven verir ve daha fazla işlem gerçekleştirmelerini sağlar.

**- Granular Control:** TLS gelişmiş bir alert sistemi sunar.

**Dezavantajları**

**-High latency:** Diğer birçok güvenli şifreleme yöntemiyle karşılaştırıldığında TLS daha yüksek gecikme sağla

**-MiM attacks:** TLS'nin genel olarak güvenli olduğu düşünülse de, TLS'nin bazı sürümleri hâlâ man in the middle saldırılarına karşı savunmasızdır.

**- Platform Support**

**- Implementation Cost:** Implementing a TLS certificate isn't free

**- Network Complexity:** Ağ mimarisindeki karmaşıklık

SSH

**Avantajları**

-Güçlü şifreleme

-bir çok platformda çalıştırılabilir

-VPN olarak kulanılabilir

-bir çok authentication metodunu destekler

- Data Integrity

- Secure File Transfer

- Port Forwarding

**Dezavantajları**

-trojanlara karşı koruma sağlamaz

-DoS saldırılarına karşı zayıftır

-dinamik port desteklenmiyor

**AĞ KATMANI**

**Ipsec**

İnternet Protokolü Güvenliği, yani IPSec, internetteki veri paketlerini doğrulayan ve şifreleyen güvenli bir ağ protokolü paketidir. İki önemli rolü vardır: Şifreleme ve Kimlik Doğrulama. IPSec iki modda çalışabilir - taşıma modu ve tünel modu. taşıma modunda, IPSec iki ana bilgisayar arasındaki trafiği şifreler. Burada, IP başlığı için değil, yalnızca veri paketi için şifreleme olacaktır. Ancak, Tünel modunda, IPSec iki alt ağ arasında sanal tüneller oluşturur. Bu mod, verileri ve IP başlığını şifreler.

**Avantaj**

**-Transparency:** Son kullanıcının IPSec veya yapılandırması hakkında endişelenmesine gerek yoktur.

**-Confidentiality:** Herhangi bir veri alışverişi sırasında IPSec, gizli verilerin güvenli bir şekilde aktarılmasına yardımcı olan genel anahtarları kullanır. Sonuç olarak, anahtarların güvenliğini sağlamak, güvenli veri aktarımı sağlar

**-Uygulamadan bağımsızlık:** IPSec güvenliği, ağ katmanında uygulanır. Böylece kullanılan uygulamalara bağlı değildir.

**Dezavantaj**

**-Wide access range:** IPSec tabanlı ağda tek bir cihaza erişim vermek, diğer cihazlar için de erişim ayrıcalıkları verebilir

**-Compability:** IPsec, multi-protocol ve multicast trafiğini desteklemez.

**- CPU Overhead:** Sunucudan geçen tüm verileri şifrelemek ve şifresini çözmek için oldukça fazla işlem gücü gerektirir.

TEST\_A\_B

unsigned char key\_128[16] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16};

unsigned char key\_192[24] = {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24};

unsigned char key\_256[36] = {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, 32, 33, 34, 35, 36};

AES ENCRYPTION TEST-128bit key

Plaintext: Hello World Test

ciphertext hex: ef d8 23 1d 2b f1 60 72 8f ea 6d 62 5b 26 54 2a

ciphertext ascii: #+`rmb[&T\*

decrypted hex: 48 65 6c 6c 6f 20 57 6f 72 6c 64 20 54 65 73 74

decrypted ascii: Hello World Test

AES ENCRYPTION TEST-192bit key

Plaintext: Hello World Test

ciphertext hex: 24 2c e8 88 38 bc 21 96 1c c8 b8 98 d7 75 d3 04

ciphertext ascii: $,8!ȸu

decrypted hex: 48 65 6c 6c 6f 20 57 6f 72 6c 64 20 54 65 73 74

decrypted ascii: Hello World Test

AES ENCRYPTION TEST-256bit key

Plaintext: Hello World Test

ciphertext hex: 17 be 8d d7 d9 05 38 16 3e 07 d6 63 fa e5 b0 8d

ciphertext ascii: 8>c對

decrypted hex: 48 65 6c 6c 6f 20 57 6f 72 6c 64 20 54 65 73 74

decrypted ascii: Hello World Test

----------AES CBC MODE TEST-128bit key----------

Plaintext:

Lorem Ipsum is simply dummy text of the printing and typesetting industr

y. Lorem Ipsum has been the industry's standard dummy text ever since th

e 1500s, when an unknown printer took a galley of type and scrambled it

to make a type specimen book. It has survived not only five centuries, b

ut also the leap into electronic typesetting, remaining essentially unch

anged. It was popularised in the 1960s with the release of Letraset shee

ts containing Lorem Ipsum passages, and more recently with desktop publi

shing software like Aldus PageMaker including versions of Lorem Ipsum.

Ciphertext hex:

1bd5cb13e9b12f2dd54448cb730dba542fb27f4068744cce3969ac4a25011443

98d3b66a956b84bbbb3cc910291d1d7081e5f6d4f3d6b3b89eb873445a8ec7fd

3460121cd86e30d3a87c8904a520ebb6e26c7885961141be209b6d0766d034d1

43f0e2d365430f14a11980748ae97b183ede64d8d65de627b862bc13f545b0b4

ec460bb06049a210c3db48ff2f25227bd374d6bfccad628ae4caff05cb94afe2

494ab26c4d7febe51ed84fae6bbb4c5e407e4d20ce76f48f65ec1d7c718cca22

556b5116ebaf7938f41def9613282fe37afbdad6866f0471e7e332fe2794a649

deac12668cf6c6929426064d83e1de0ebd6cccbaed8d0fe17789ec11b65690e5

fbe4e504883b05ae3914b60c8c81c19f94785649bcf299d7905a9ac74f6bb6ad

020ad2bee0f53ddd38063669defbcdf0c733fd183cd20a9bf1a8115db56ce383

c51eeb9143dfe252938a8c2a40a7e20de1559e195996cf7f98956b32064ef64e

bc9facb0f787026489e2760c7d311437e3ea06760d81e4312a4dd31e7ab541f0

1ca22a9ece8093d32127cb4a2b7d3fa570a7c191760b127e33cdff1511505881

1de150a86f1b4038b6809878655d1cab8c2af82f3524556db081e4832e640a19

b40aae276ae2d3d370a7bdaa5e290455d422463deb5701c9220a4bc60397685a

4302893f7b94c44d702fd58ea958baf085dc68f2a0a7f1163931aba37972f230

105bf0efa24434fd36f62c955d2b13f154789f5219645eaa24e16c6a9cc15c47

7e559416b7ac960cf4b5557efeea72652501fecd3ef3345d18c5112b95ecc0eb

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

----------AES CBC MODE TEST-192bit key----------

Ciphertext hex:

a58a40a07e296ad0c6e57d9767d7ac0955bb6b53f9b9242995ce5cb6aa67b74f

e5e5caad6069527047d44e95d2b971df44b80ea3b8740a1e227e64207c3f583d

7605f78950711722fd9a6e779ffe32019f0fdc150027cd7df1ce93099a28a781

1443db36d6cef5b9e141d87fe5326c2689b206882282cba537739027b1801b03

074f6da6a7a524ccd783b5e617063957f0d220eb5a7a026ae83d7ae5f31f42be

56afd8717df155c4f161730b1edb30960e525504e43d6163adb0a3bd2d164b7e

39950622d67e983995f41f311096e1c1aa7b0cdfa16bb9ca8e6903a7c0f2f6b5

a6c2d63f1e7e48f21c34e92ef8d1fb55347d93ec09cd859118e66230e95ec9a4

35fe1f62b0bed96a54ccfbdfdfaaffc37e5064c5c0d5cee79ad20e263e058526

44fc4b36dcfdb8212279170fb1c75737320c4a074ad0ef48f219d8d63abb10e6

4c88e4f86355b08734d8f0a547afa03bdb2af99c1c6e2d5f13894079f30dcb88

e92694a1fef79e2b5fdb74bb4a309d27e91f015901ffb7475da42d6ba4b043e5

fad7e910de2d54bfbd1e081424e17d272ca68ddb7407b67281b69fc52fb963f9

91a7cde085e6a8e5ce245331f83b2a67894dbe96fd7784aa0dabbab7e2f07712

0944a23d7dac74d588a644d57f3238fb95beb0551e15ce317a5cf2f6dbb30e31

439a7e3baf431f716a7f53c6c5056bf9e00008c2cc558cf59f0ae60905bbe2b7

af8625f1d3ccb1577f0de0eb431a0fb8778c1690da68c1edb0e6b70931dc164c

4b9519adb842eee62f560204a195530e174667451f31656dc4d9d1d1dac673ed

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

----------AES CBC MODE TEST-256bit key----------

Ciphertext hex:

9decaebd660499f6b4029d8f7c0f7b853af51c3393c540d3f2d3355b60339ce8

ba1a29443e197336e71ade491e8a64c440ab9f7017980273c70388ac2bcfb0d1

1e7b7a876e26de73e631bd3e4ab4fcb1ea8dc83a761525a9f9365b6798b1432f

fed8cf22040c200b4a9a09ebcbd0d7efcac26ceca1de1b441b17be4441c8fc49

61a00e5591b84cdad4e3e9dd40498d697e3c3f2fada531fd2372e19ee8f03f54

6d19d1fe17ea8ca5e32fc92fea99bbfc900b3accd794e19f72e4bc401adda4b9

1d995e6affba61643adb61ee6b8b5cbe932ff9b1aea600fac8a9922cd3a4bfb9

e312eebf86db5acc7c516197ac960d1ab1d305048264e1dd68d274f940b9c431

f8a602e16233072b80c00898b9ce7cbcc9f5f80b1a95bf1f360a67f3bb3027d5

5b6a3c3b731e7cf874b6a0cb99bde6afe1996cdeb5e2bce8c88ddbdbda347f1f

39f6eebe9398e834ecfabbcf875192088786b0c3ff360608d9bde01b21c90ddf

9793a7b17148e580eeea6a0abaa81c001cce502c4ed8ad595bf52c53e5194d16

907ac21f9be41710d83af130cbdb9c71eb496fbd5a4cdcfef5c621659758af72

b72ddf6b6b02f08b55d86e9f6305b2dcdf9f5369b749ec8d8869de1f6aefcaa1

4a79368498bcd6b9dd86d4d5d0e418b7a509b1d85515d75afcb8d7d2d70478fe

78a2b82e2ab1f1ee759560942f986de1a48043930b0c24d2f7b4db583bdac084

3ab35075f084eff411704db9f332299047e86d9c80ad7873245048ccc9237813

8ca09857c814ae2d6614b417b1157cc7eeb031abf4405a03803bb98db64a51af

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

----------AES OFB MODE TEST-128bit key----------

Plaintext:

Lorem Ipsum is simply dummy text of the printing and typesetting industr

y. Lorem Ipsum has been the industry's standard dummy text ever since th

e 1500s, when an unknown printer took a galley of type and scrambled it

to make a type specimen book. It has survived not only five centuries, b

ut also the leap into electronic typesetting, remaining essentially unch

anged. It was popularised in the 1960s with the release of Letraset shee

ts containing Lorem Ipsum passages, and more recently with desktop publi

shing software like Aldus PageMaker including versions of Lorem Ipsum.

Ciphertext hex:

979ef674439958662a04468fa6818b57d5f6ff9221f924fc1c2be7cecab31705

f0cf27a7719b877a166171ce315981f06afa19e6d37fd88d2c88dfccac8ab760

0a82981b5e693809d95f55f6530f0c07dc1d31c901be0f4bf4712e2655d3a25e

db50c602db557e41c90f7166ea24204e47cdc4855fde9982f96b5b8f42edd5cb

9c671c2678616727152e59cf0c8271219f6b5652cf8ac8c7b3d0efcaed91458d

0d9630456b4117f83f4d1b89666b70a5a6dd1a26fd29cf4c54c8703e00f2fb02

e6d1f0aa30039c5e9a80206b77441327401a83416d4ae81f11e9e1a0448811a5

c520989b5fc4ebeda0afcabcb42b8f4e1869fb50328ac26cc406f214f94965bb

12a9caa32d7ed79c7bb44352c902a52d611dae01e944021b5520a2e5300e1d28

3827b887e078a594bc8dc27886200ac0d120428d880a7d7969b0d1ef7464b025

1a45140f82819086b9a35a89c0078c9d5301f9133d0eb1487f76269fc731c9c0

06738b1f7e2bb5de845bb934ed95e2eb38408d95791cf447e2fea08cb8c4504b

2e7ac989be081929565efbc45e8ef9cc15227e88c92b3fff97d9d13a82a031f4

81ddfb21decb6160538bf302f23f255504ea62188a6f0ca17f18791c0b6b97cd

6eb0bdbe4a784cfdaa204acb3728e57620e728c57f7a43afa2a4abcd0b3f41ea

aa396459d7d73239981f84307bb58bdc787a1d654b4db15307cd5590952fca0c

279c82c0194447fa452d5a1909954073a186b88bb42b82121efc614bb414bbde

998075406dcc938e704087ffc6bc27895fefd45403b4ca379c35f5e0bc3742a6

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

----------AES OFB MODE TEST-192bit key----------

Ciphertext hex:

f1373e0ea173dcda947a890828bf99662cad6264aee9b88847c53f50c1a7eeb9

edc3ee5622b2e121c617f2548cca473e570ccbb35e43a0e75313f5b5f7a5f8f9

06544fd1443a0a2d31a6cb93d63a3cf2e685bd8925c928851dbc8016d656377a

a4724412a0f6a25bfa4b9619e577a975f99e741dbe7020cc24303fef2f2c4b70

f171697227f1634cc692d28a65088fc132cc81fb37e305c648d31af9c68d84a9

8439c5d7c5dd5c97135b81f81896123a887ad9e94cb9fe9bd4abcb1fee764c3e

1e396a33fffc80a4b3354bdf65d875e6c274ae0c93761946b85533ef1f4c1e87

dd89abaa95ee18b938a548217fccce47bb6494b8f47e74901dbc2e319d4c021f

9bf0cfb1bb12775e4db1c4dc79f5e76dd1efb16f8ee768f692ab13f22ea4f891

5b0f5eff2ab54a9382506575de745e60ec7f851b930b3f8dcc013516205b90d2

71b25b322c52bb933da27ecc61bb2d1a98cd80d7d001bfa4d682cbd9b2210f19

7b2a654bd4532d36dc244f736bd8ec9fe88cffef72e3846d2f75e515ce713207

60821bbe88d30f27e088e9bf8603e86a8cd5276044af523e4800401049f3dfb4

baad202ad1a26df3e08cca6308d77a38192f810db11f6acd269fd635d44c3db8

0eb73f6091d0854a4cbd9c85ad5cc5b540947ffb35945503d72129c914903e5e

fec9beb045d41512e5bf77bbb121a8431a23ff0f10bd4edf78009ba0093b3051

3346f589ae93d53e0c137e3cc9aa8a8b528b8bd84762c488f8e745466feeae51

dc5bd2add4e745d0d2859858db0e5828a15cb430f70f3037b201df1031a5f954

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

----------AES OFB MODE TEST-256bit key----------

Ciphertext hex:

eb5327130b5b3233d14ff2f959c6662ee3f4be8bf343a6dcfe1e9efee43db84e

09e14b721026d63c32a22a866768ae7d7a71d0c2916237c33298d52b6fc6bd0e

15fe65d9ada1ea84f64374c45af012facf6cfed7ea0def8266c18a8c2f63db7f

f78083380883afe6ea4e88a9084cafeec384c9382466bed05e740a4543c7c029

04695ce34757830150a04a2f2f3e586c83457cd30cdabce4bf891d6a65ebde6e

db1f59ead46f107940fe5a5641f920e0d8d967c30f1b179fbe5fca590af26ef8

be59685d39a934bc2b80ac274ed8594746f730c4637cec47f1f55267ba422959

f054c7a53b1d3d2eaa75817e693c499fd0e3cd071f24b99733676b752099ac6f

5104c7db6452e231541e3a2138d4baddbffdc468d97cd25fea27bad222e3e64a

640c43728ef92a37ba624bbbdd1f9e41aba9c186903be125c4995ef1da8e0478

0105c1f86dd28af87a2412c8180383ea0eb61c1abddc42f3d8780457ba38c6e2

07e7161ce6bf728bc97fd19769f706a33249904178dc43aa9ef15454cf05ac29

229fbe10c7b8886ff290020ae124d018c2fb17a8210ff09aa624b5e669777a5f

dec660ec70cb5c7ad82819e3d5b1ee0cdc54b75ea00ad3fb1c6bdb6acbba6520

edda5049fc812cf281dd859cb947f34acf5b357fc30f81068fb8354b184f415e

aa0e7c18af52c667d017aee18852c696935e5ff6aa8c200a10d0a0787e66eae3

2594680ee8e470bcb2aec56516649b865a9906e2e857b518dc729d67c4c14997

af50f4d77a0c2ac6b84b585fb6990a4312ca38dff5ce302ba0e44e974d6e5d5e

Decrypted ascii:

Lorem Ipsum is simply dummy text

of the printing and typesetting

industry. Lorem Ipsum has been

the industry's standard dummy te

xt ever since the 1500s, when an

unknown printer took a galley o

f type and scrambled it to make

a type specimen book. It has sur

vived not only five centuries, b

ut also the leap into electronic

typesetting, remaining essentia

lly unchanged. It was popularise

d in the 1960s with the release

of Letraset sheets containing Lo

rem Ipsum passages, and more rec

ently with desktop publishing so

ftware like Aldus PageMaker incl

uding versions of Lorem Ipsum.

TEST\_C\_D

Başlangıçta dosyanın içeriği :

(aa.txt)

Lorem Ipsum is simply dummy text of the printing and typesetting industry.

Lorem Ipsum has been the industry's standard dummy text ever since the 150

0s, when an unknown printer took a galley of type and scrambled it to make

a type specimen book. It has survived not only five centuries, but also t

he leap into electronic typesetting, remaining essentially unchanged. It w

as popularised in the 1960s with the release of Letraset sheets containing

Lorem Ipsum passages, and more recently with desktop publishing software li

ke Aldus PageMaker including versions of Lorem Ipsum.

HASH eklenmiş hali:

added hash= cc7e245ca8470980e996357692bf8bad

Lorem Ipsum is simply dummy text of the printing and typesetting industry.

Lorem Ipsum has been the industry's standard dummy text ever since the 150

0s, when an unknown printer took a galley of type and scrambled it to make

a type specimen book. It has survived not only five centuries, but also t

he leap into electronic typesetting, remaining essentially unchanged. It w

as popularised in the 1960s with the release of Letraset sheets containing

Lorem Ipsum passages, and more recently with desktop publishing software li

ke Aldus PageMaker including versions of Lorem Ipsum.Ì~$\¨G €é–5v’¿‹­

Hiçbir değişiklik yapmadan kondrol ediyoruz->

Graphical user interface, text

Description automatically generated

Dosyanın başına sadece bir karakter ekleyip tekrar deniyoruz->

(dosyanın son hali)

aLorem Ipsum is simply dummy text of the printing and typesetting industry.

Lorem Ipsum has been the industry's standard dummy text ever since the 150

0s, when an unknown printer took a galley of type and scrambled it to make

a type specimen book. It has survived not only five centuries, but also t

he leap into electronic typesetting, remaining essentially unchanged. It w

as popularised in the 1960s with the release of Letraset sheets containing

Lorem Ipsum passages, and more recently with desktop publishing software li

ke Aldus PageMaker including versions of Lorem Ipsum.Ì~$\¨G €é–5v’¿‹-



Hash fonksiyonu olarak b’de gerçeklenen CBC modu kullandım. 128 bit AES ile şifreleyip dosyanın sonuna ekledim.