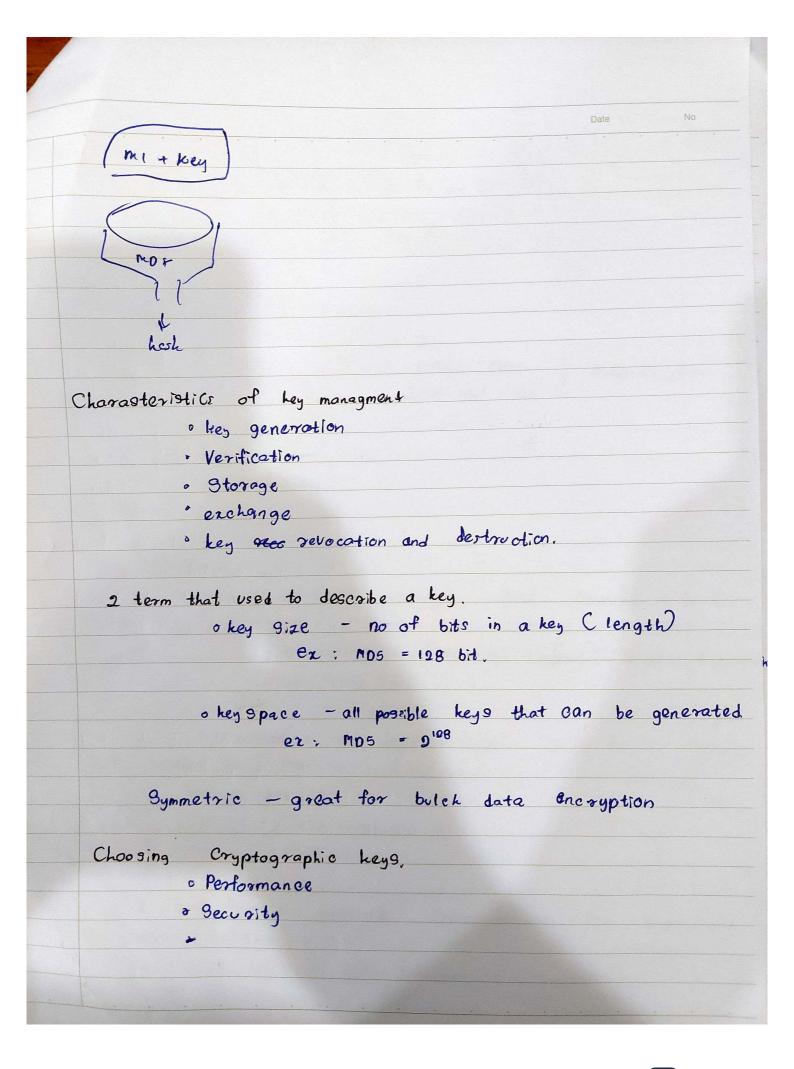
ProMate



Cryptography III IC9 lec 7 Symetric encryption keys · DE9 (Weaker) the classe 83080 to fined leadth pe confidentiality · AES (Stronger) o each black 64 or 108 bit · Confidentiality may depending on keys, in Symetri c key alway9 give confidentiality. se test I doubt hid act to 138 IP sec - Network Layer Confidentiality 391/TLS - Session Layer Confidentiality Secure messaging - application layer confidentiality o encount plan text Symmetric key Algorithm. Same key used to enclose, (shared Secret key) okey length 80/256 bit o Speed o DE9 , 3DE9 , AES Asymetric key algorithm. o public key algorithm o hey length 512 - 4096 bits o have private and public key · public her shared private key not. ORSA DH **ProMate**

2 type of Symetric Encoyption techniques

- · block Ciphers
- · Stream Ciphers,

Block ciphers, (strew)

and encoupt an parts at once.

Simetale encouption keys

o each block 64 or 128 bit.

o Confidential to may dependent on tog the

Ex: $OES \rightarrow 64$ bit block

AES \rightarrow 128 bit block / 1991 236

Stream ciphers,

time. C character by character).

Can be faster than Block ciphers. (Data transit)

Ex: A5 -used in mobile communication.

RC4

Compane block, Stream ciphers bared on Speed of enc.
Size of output, and Security.

ProMate

Speed data at very Farter Stone Speed data at very Farter Stone Some farter Some farter Security S				Date No.
date at trois glove factor Some factor Some he lorger has garden is truted by Cryptographic community of trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import restrictions Octa encryption Standard C DES) -not used these days only so bit key length actually 58 bt convert it to 84 bit.		Blook Oil	pher	Stream Cipher
chosing an algorithm o algorithm o trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import restrictions Octa encryption Standard C DES) - not used these days only sa bit key length actually 58 bt convert it to 84 bit.	Speed	data at vers	faster	s Lower 8000
Secure that Secure that Stream Choosing an algorithm algorithm is truted by Cryptographic communitation trusted algorithm or not. algorithm or not. boes it protect against brute-force attack. boes it support Variables and long length keys algorithm or not. boes it have export by import pertrictions Outs encryption Standard C DES not used these days only 64 bit key length actually 56 bit convert it to 84 bit.		data at troi	glove	faster
Choosing an algorithm a digorithm a digorithm be algorithm c digorithm c trusted algorithm by Cryptographic community o trusted algorithem or not. boes it protect against brute-force attack. boes it support Variables and long length key. Ones it have export by import restrictions Outa encryption Standard C DES) not used these days only 64 bit key length actually 56 bit convert it to 84 bit.	size of	noily com "	+1	d study stable ton - 803
Secure that Stream Choosing an algorithm o algorithm is trusted by Cryptographic community o trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import pertrictions Octa encryption Standard C DES not used these days, only 64 bit key length actually 56 bit, convert it to 64 bit.			Somecon	Some
Choseins an algorithm o algorithm is trusted by Cryptographic communition o trusted algorithem or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import restrictions Octa encryption Standard C DES) not used these days only sabit key lengual			he lorger	- 395
Choseins an algorithm o algorithm is trusted by Cryptographic communition o trusted algorithem or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import restrictions Octa encryption Standard C DES) not used these days only sa bit key lengual	San H		C. N	
Choosing on algorithm o algorithm is trusted by Cryptographic communition trusted algorithem or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import pertrictions Outa encryption Standard C DES) not used these days only sa bit key length actually 55 bit convert it to 84 bit.	2007.0			
o algorithm is trusted by Cryptographic communition trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import pertrictions. Octa encryption Standard C DES) -not used these days only 64 bit key length actually 56 bit convert it to 64 bit.) creon	
o algorithm is trusted by Cryptographic emmunition trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length key o Does it have export by import pertrictions Octa encryption Standard (DES) -not used these days only 64 bit key lenguations				
o algorithm is trusted by Cryptographic emmunition trusted algorithm or not. o Does it protect against brute-force attack. o Does it Support Variables and long length keys o Does it have export by import pertrictions Octa encryption Standard (DES) -not used these days only 64 bit key length actually 56 bit convert it to 64 bit.				
actually 56 bit convert it to 84 bit.				is trusted by Crupto graphic community
actually 66 bit convert it to 64 bit.		0	algorithm trusted all boes it pr Does it s Does it have	gorithem or not. Noteet against brute-force attack. Bupport Variables and long length key Report by import pertrictions
		0	algorithm trusted all boes it pr Does it s Does it have been deador	gorithem or not. Noteet against brute-force attack. Bupport Variables and long length key Report by import pertrictions Of CDES
		Oota encryptic	dgorthm trusted all boes it pr Does it have n Standar not use of Convert	gorithem or not. Noteet against brute-force attack. Bupport Variables and long length keys a export by import pertrictions and CDES) and CDES
		Oota encryptic	dgorthm trusted all boes it pr Does it have n Standar not use of Convert	gorithem or not. Noteet against brute-force attack. Bupport Variables and long length keys a export by import pertrictions and CDES) and CDES

	Date	No
OFS operation modes,	in	
OES operation modes,		
о ЕСВ 13 13 13 13 13 13 13 13 13 13 13 13 13	s to state	
· CBC		
ECB - not suitable to use large datas.	encryptions	
CBC -		
Edward that I was		1
e de la companya de l		
on three classes	(E) 1 (40 T 20 A **	
e doorthm is tricked by couptagoople come		
as too or matheone between		
o Dies it parted against boots fore attach		
a Does It have Expost by unpast sentengences		
peros steaded Coppe	200 m n460	
 103 to a place downed book loss to -		
that the state of	- Books	