Date. / /	Andrew Communication of the Co
3.	S. J. O. ECBAŘÍČ
TLS*= TLS]	to 是一种,是一种,这种是一种,这一种,是一种,
τp*= πp-1	经验。有代证价值减少证法。24-dk(9;)
可靠到那些自己(自)出现的	、差界要性對議。[大學和 X = dk(B) b3 新宗结果,其资
3.2	1进分别的是公司
假设密文经过N轮加	密尼为(Ln, Rn) (表別 8 10 (6)
解密从最后-轮开始证	向操作, <u>Max. (may o = a a. 所有的名字</u> 数类形式的
:加密时最后一轮	= (Lv, Rv) = (Rv-1, Lv-1+F(Ru-1, Kv))
: 解密第一轮: Lv+	= Rn+F(Lu, Ku), Ruy=LN
::同理,逐轮逆向持	操作可以完全恢复明文
•	大学工作工作
3.3	C Cpc tig 大
发明文x和密钥K的	取反为 C(X)和 C(K) (1) (1) (1) (1) (1) (1) (1) (1) (1) (1
在DES的每一轮中:	是这个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一个一
轮数户的输入	是Ri和于密钥Ki。由于F由异或和置换组成,且c(RiOKi)=
	此F(c(R),c(k))=c(F(R,k))。
下一轮的左部分	Lin=Ri,在部分Rin=LieF(Ri,Ki)。
对抚反的输入	(c(Li),c(Ri))和取及的密钥c(ki);不一轮结果为:
$c(L_{in}) = c(R_i),$	$C(R_{2}H) = C(L_{2}) \oplus C(F(R_{2},K_{2})) = C(L_{2} \oplus F(R_{2},K_{2})).$
二 每一轮的加密结	果均取反后的值。《《二》(三》)《《一》)
:, y'=c(y)	指述。 (1=4⊕ Ct (4→1)
音点	· 提供提生错误行影响图: 从EUE Calga)。或语则X
Swale (The Day of the Cally A the
四语表下。此一时	人教司 X2 X2 高载台县大学集
	二、表音流。纪数功2

3.7 O ECB模式		1.8
加密:每个时	用文Xi独立加密,即 Yi= ex(Xi)	X5 75
	致分组独立解密,XL=dk(Yi)	T.p* = T.p*
二老9级生错	误,仅影响 Xi=dk(yi)的解密结果。其它	3分红少;(j+i)的解格不受影响
4. 错误分组类	&为1	1,2.
② OFB模式	(E为(Lu, Pu)	11/5000多人的主义系统。
加密·先生的	(一个密钥流S;= ek(Sin), 初始S。= IV,)	密文yi=Xi田Si
解密:重新	生成相的密钥流Si=ek(sin),明文Xi=	·y;@S; Taltan
·· yi若错误	,7又影响 从一岁,田岛,的解密结果。由于岛	;不依赖密文,后续Sin,Si
不受影响	主义的是全体是明天	二同理,连轮进向转
山错误组数	b]	
③CBC模式		\$.3
加密: Yi=	· Ck(Xi的yin),初始y=IV	发到又x和临闭口的
	xk(yi) & yin	主FS可经-轮件:
· 若y泼生	者误{影响从:Xi=dk(4)曲岁-1,少错风	X结 三人
	影响Xi+1 = Xi+1 =dk(yi+1)⊕yi, yi	错划Xin也错
	(漏响Xin,Xin,后续分组仅依赖Yi	H, Yinz, 不受影响
c. 错误组	数27(3)5月19日夏季等((3)5,(3)5)	人。萨伯承无敌
OCFB模式	$C(\mathbb{R}_m) = C(\mathbb{I}_3) \oplus C(\mathbb{P}(\mathbb{R}_n,\mathbb{R}_3)) = C(\mathbb{I}_3 \oplus \mathbb{P}(\mathbb{R}_n))$	c(lim) = c(R),
加密: Yi=	Xì⊕ek(yìn), 存放线 y。=IV	二年一於例中學行
	y;⊕ek (Y;→)	(u)o='h :-
4. 若 y 该生宅	错误⟨影响スシ:スシニyi⊕eklyi+),歩错则ン	X;错
	影响Xin: Xin= Yin田 ek(yi), yi错	
	不影响 X++, X+3, 后续分组仅依赖	Yirl, Yirz,不受影响
二错误组数	(为2	

000

No.