R6. 对称容别 $C_N^2 = \binom{N}{2} = \frac{N(N-1)}{2}$

公开祭祖·每个人玩一个属于自己的公明公开发布,保留和明代意式起一次通信 A>B都可以用B的公明加密 kis(m), B用保留的私铜融客 kis(kis(m))= m.

支幕ZN ケ茶湖。

RIS· 我认为基子数字签为的言案更适合。

解答 In media

采用MAC的方式需要向"数以干计的清晰为友一个鉴别宏明,首先分发的代价可能很高,其次将有很多用户共享鉴别密明安全旧难以保障。但如果同时用防发洞的密钥,代价将很易发。 采用数字签为的方案 只需要在互联网上发布同 加的相同的 公湖,分发代价更低,也无需恢复全企。

R23. Bob 使用Alice的公钥加密主题词发送给Trudy, Trudy 无法解析 出对称签钥

Rims Camodn

在推辑法最后 bob的 Trudy向 Bob发送一个包括所有说"推手报文的MAC. Bob 验证失败,拒绝连接.

16984 1 0 0 15 17085/375

हमर्गहरू

不可以. 因为采用3多码代替器码,加密采用3多个单码(分别)包含不同的映射信息-),并且还包含3这些单码使用的含不同的映射信息-),并且还包含3这些单码使用的资次序信息-,这款还择文本只能确保每个多用出现。至少一次,程以破解加密方式。

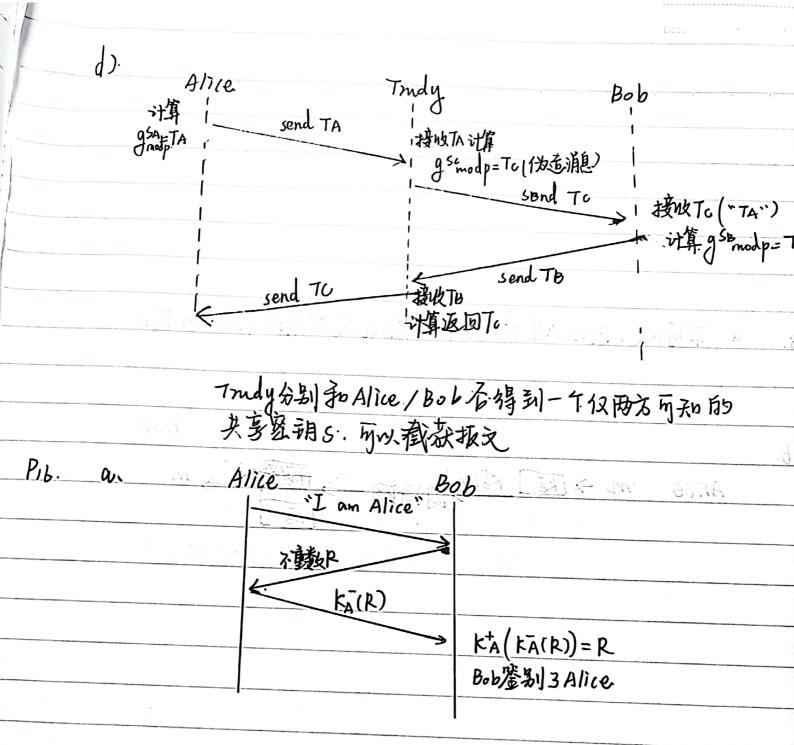
 P_7 . P=3 q=1 n=pq=33 $3=2\times10=20$ 这样 e=> e和3 3意 选择 d= 7 2/mod 20 = 100 1 1 kt: (33.3) k-(33.7) 京相, 分表约约里位一 15: 170859375 13823543 dod (in plant torday also sign Bob The DELY No 明文C 茶文m= camod n 16384 井 170859375 4 823543 彩 . .

明文化 Ce/e=3). Cemod n 花文m m^d md mod n 64 2/512614111 3375 4782969 343 62 48517 d: 001008 h) 0: 01111 > dog: 00/00&0/11/0011/ 9: 20111. 明文6 m= 4583. 因为 c = (me modn) d modn = m. 放m应以于 n. 因为自己确实没有能力找到一组这么大的统胡,上网学4搜索到 P=43 9=107 n=px9=460 8= 4452 e=61 d=73 memod n = 402=0 m odmod n = 4583 = m. of your (aporage of the of I down to some by a down as We - S n= R9 = \$ x, J= 2 +5 | Joan = 2 = 9 bom P8. B= (p-1) x (9-1) = 4x10=40 (= about a) b. 因为 e=3<n=st·, e和z至意 并且通常还存的交通的公钥 c. 五样 d= 67 exd==40.20 mod 8=11-AT (0) The y sh mode = 2 mod 1 d. Fre= 83 mods 55= 107 (Long 6 12) = 200

a. TA = SA mod P TB = SB mul TA= SA & nud p. TS= SATB Wood p= SASB modp) wwd p S' = SBTA nwdp = SB (SAOnidip) mudp 又有 <anual n)d mod n = adnual n. S= (SA mod p) Sp nod p mod p = (SA mod p) mod p

S' = (SB mod p) SA mod p mod p = (SB mod p) (SA mod p) mod p

TA = g SA mod p TB = q SB mad p TA = g SA mod p TB = g SB mod p S = 7 5 A mod = g SASB mod (gS b mod p) SA mod p = (g SASB mod p) mod S' = 7ASBmodp= (g SAmodp) Strodp: 1 g SASBmodp) mid p 5 b). TA = Sagmod p = 52 mod 11=25 nod 11=13 7B = SB9 modp = 122 moder (== (-) C) S = SATO modp = 5 model = 5 5 = 60 TA modp = 123 mod 1 = des b). TA= gsamodp = 25mod11=10 $TB = g^{SB} \mod p = 2^{12} \mod 11 = 4$ c) $S = (g^{SASB} \mod p) \mod p = 2^{16} \mod 11 = 1$



Alice向Bob分发公钥的报文被Tondy拦截,Tondy向Bob 发送自己的公钥 片并声称"I am Alice",之后Tondy 收到。 Bob发送的不重数尺,用片加密后发送给Bob, Bob 解码 后认为认证成功。同样。Tondy也可以哄骗 Alice声称"Bob" 就可以获知甚至修改它们通信的内容3。

	THE STATE		
10.0%	1	AT Jugor	N. Carlotte
	ALUGER		
to the state of the state of	TAN P		
("AT") 01 20 (2)			
SI Explana & All			_
A Control	WI WILLIAM	之始在的信息	和树志。
P18. a. 不可以,因为没有提供	任何Alice.	10 NOV PL	
P18. 4. 不可以人,因为以内的人门			
有特别一下仅限品可知的	Alice / Bob	af 19 8 home,	l2 1
1-1	机外截容数	大多级祖子。	Bob-
		(Fallem)_	. m
Alice m → [kē] Kēl!	为因持网一	1	>
	53118	Ke	
	\$	不達起戶	
	(4)		
$E_{A}(E_{A}(R)) = R$			
Bobile 2011 BAILE			
16 - 22 - 22			
the Imakastay Tondy 10 600	于自计为表文		
alle Jak Trudy 1X 3/6_	1 . 62 Z	M Bop II Was	Alice
被Tondy 对意,Tondy To Bob m Alice: 二后 Tondy 以到 最后发生给Bob, Bob 解码 与可以或编 Alice 声说。Bob	12 - We at	的会租任重	这些自己的
1 0 5 5 5 11 6 5 M 9 W	FD KT DOL	らえ着後と	8 2 V 1 0
BANK WHAT AILLE FISS. BOB	HANT X	- Carrow L. A.	DOD KIEL
新国权政府的中央。 这可以成都 Alice 声说。Bob	D T	Tal & Ma XII	To W. to W. V.
	W. Ciram	如其至人家	die en Pa
		1	VII. VIVIL OF

P19 a- 京产

- b. 128. IP地址: 216.75.19 4.220
- C. 204+79 = 283.

d 3

e. 包含用 server 公羽 加密的 多 密钥

f. bc.

- 子客户端·发送3·3条接收3:3条
- 九. 服务品端:发送34条接收33条