```
Also possible to use RSA to build PKE:
"Textbook RSA" (How NOT to encrypt): Consider the following candidate of a PKE scheme from RSA:
      - Setup: Sample (N, e, d) where N=pg and ed= 1 (mod ((N)). Output pk= (N, e) and sk > (N, d)
      - Encry pt (pk, m): Output c 

me

Correct since

Cd = (me)d = med = m' = m (mod N)
Correctness follows from correctness of TDP.
How about security? NO. 1. RSA says that computing eth voit of random element should be difficult
                                       1> Does not apply if messages chosen adversarially (e.g., semantic security definition)
                                       L> Does not say anything about hiding preimage (e.g., Xe can leak information about x so long
                                          as leakage is not sufficient to fully recover x — this is a weaker property than full indistinguishability)
                                2. This scheme is <u>deterministic</u>: cannot be semantically secure!
                                                                         > in fact, vulnerable to message - recovery attacks in many
 NEVER use textbook RSA!
To use RSA to construct a PKE scheme, we will use a similar strategy as in the FDH signature construction:

- Setup: Sample N=pg, e, d where ed = 1 (mod P(N)). pk = (N,e), 3k=d
                                                                                                     Scheme is randomised!
   - Encrypt (pk, m): Sample x = 21
                        Let k \leftarrow H(x) where H: \mathbb{Z}_{N}^{*} \rightarrow K is an (ideal) hash function and K is the key-space for an
                                symmetric authenticated encryption scheme
                      Compute y \leftarrow x^e and ct \leftarrow Erc_{AE}(k, m)
                        Output (y, ct)
   - Decrypt (sk, ct' = (g, ct')): Compute x = y^d \pmod{N} k \leftarrow H(x), and output m \leftarrow Dec_{AE}(k, ct')
This is an example of hybrid encryption or KEM: y is used to encoqualiste the key and ct' is an encryption under he
Theorem If the RSA assumption holds and H is modeled as a random oracle, then the above encryption scheme is semantically secure. [In fact, this scheme is CCA-secure in the random oracle model]
<u>Proof intuition</u>. Given a ciphertext (y, ct') and public key pk = pp:
                     - Adversary cannot compute x from y (by RSA - observe that x is uniform over ZX)
                     - Adversory cannot evaluate H on x, so k is uniformly random and hidden from adversory
                     - Semantic security follows from semantic security of symmetric encryption scheme.
```

In practice:	: Most widely-used standard for RSA encryption is PKCS1 (by RSA labs) -> Has shorter ciphertexts if we are encrypting a single ZN element (no need for XEM + symmetric component)
	(helpful if PKE just used to encrypt short token or metadata)
	General approach: suppose N is 2048 lits and we want to encrypt 256-bit messages
	be will first apply a randomized padding to m to obtain a 2048-bit padded message
	PKCS 1 podding:
	(mode 2) 00 02 non-zero rondom bytes 00 m
	16 bits share s t
	t-bits long
	Encryption: Compute mand - PKCS(m) and set C - mond [i.e., directly apply RSA traphon permutation to padded message
	Decryption: Compute mpod - col and recover on from mpod message
	In SSL v3.0: during the handshake, server electypts client's message and checks if resulting mond is well-formed (i.e., has valid PKCS1 padding) and rejects if not -> scheme is valurable to a chosen-ciphentext attack!
	-> allows adversory to earesdrop on convection
	Devastating attack on SSL 3.0 and very hard to fix: need to change both servers + clients!
	TLS 1.0: fix is to set me Zn if decryption over fails and proceed normally (never alect client if
	godding is malformed) - setup fails at a later point in time, but hopefully no critical information is leaded
	Take-away: PKCS1 is not CCA-secure which is very problematic for key exchange
	Absence of security proof should always be troubling
	New Standard: Optimal Asymmetric Encryption Padding (OAEP) [1994] (Standardized in PKCSI
	→ Can be shown to be CCA-secure in random oracle model) version 2.0

Now that we have digital signatures, let's result the question of key exhange (with active occurry) Alter 3° 3° 3° 3° 3° 3° 3° 3° 3° 3° 3° 3° 3°																														
Alice 9x 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	No.3 +	hat we	. ha	re 1	latioi	Sign	~4.4	1 25.	kt's	rt sli	s) + 4z	he.	Ques	tian	ર્ય	ko.	ı ex	chan	De.	(ພ	th a	ctive	820	_ሆ ራትላ	•)					
In addition, should guarantee that one compromised session should not affect other housest sessions - Alice - Eve should not compromise security of Alice - Bub Authoriticated key exchange (AKE): provides security against active adversaries - Requires a "root of trust" (certificate authority) - we need some binding between keys and identities Alice, phalice CA (one-time setup, at least for duration of validity period) - the cartificate binds Alice's public key phalice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authoriticate) - Pablic key (public key for subject for signature scheme) - CA: deatily of the CA issuing the certificate - Validay dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate - (usually several hundred authorities)	,				.g.,	20		D. L.			<u> </u>	• —	7		0,		1	(5					- /						
In addition, should guarantee that one compromised session should not affect other housest sessions - Alice - Eve should not compromise security of Alice - Bub Authoriticated key exchange (AKE): provides security against active adversaries - Requires a "root of trust" (certificate authority) - we need some binding between keys and identities Alice, phalice CA (one-time setup, at least for duration of validity period) - the cartificate binds Alice's public key phalice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authoriticate) - Pablic key (public key for subject for signature scheme) - CA: deatily of the CA issuing the certificate - Validay dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate - (usually several hundred authorities)		<u> </u>	11·ce		g ^x			מפכו																						
In addition, should guarantee that one compromised session should not affect other housest sessions - Alice - Eve should not compromise security of Alice - Bub Authoriticated key exchange (AKE): provides security against active adversaries - Requires a "root of trust" (certificate authority) - we need some binding between keys and identities Alice, phalice CA (one-time setup, at least for duration of validity period) - the cartificate binds Alice's public key phalice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authoriticate) - Pablic key (public key for subject for signature scheme) - CA: deatily of the CA issuing the certificate - Validay dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate - (usually several hundred authorities)			•		98		→				+	comp	letely	luv	moj	ole 1	to a	n a	ctive											
In addition, should quarantee that one compromised session should not affect other housest sessions - Alice - Eve should not compromise security of Alice - Bob Authanticated lay exchange (AKE): provides security against active adversories - Requires a "root of trust" (certificate authority) - we need some binding between lays and identities Alice, phase CA (one-time setup, at least for duration of validity period) - the certificate binds Alice's public lay phAlice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authanticated) - Pablic lay (public lay for subject for signature scheme) - CA: identity of the CA issuing the certificate - Ualidity dates for certificate - CA's signature on certificate - CA's signature authorities and their respective pablic lays (usually several hundred authorities)			/	-			Ī	7					net	sock	ad	1880	red .	that	Cov	· int	ercep.	t an	d i	iject	pa	ckets				
In addition, should quarantee that one compromised session should not affect other housest sessions - Alice - Eve should not compromise security of Alice - Bob Authenticated key exchange (AKE): provides security against active adversories - Requires a "root of trust" (certificate authority) - we need some binding between keys and identities Alice, phates CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phatice to Alice's identity - Certificates typically have the following format (X509): Subject (entity being authoriticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate		429							xy		J						Ľ													
Althoriticated key exchange (AKE): provides security against active adversaries Requires a "root of trust" (certificate authority) — we need some binding between keys and identifies Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phase to Alice's identity Certificates typically have the following format (X509): Subject (entity being authoriticated) Public key (public key for subject for signature scheme) CA: identity of the CA issuing the certificate Validity dates for certificate CA's signature on certificate the browner and operating system have a set of hard-code certificate authorities and their respective gablic keys (usually several hundred authoritics)		0 `	•					,	J																					
Althoriticated key exchange (AKE): provides security against active adversaries Requires a "root of trust" (certificate authority) — we need some binding between keys and identifies Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phase to Alice's identity Certificates typically have the following format (X509): Subject (entity being authoriticated) Public key (public key for subject for signature scheme) CA: identity of the CA issuing the certificate Validity dates for certificate CA's signature on certificate the browner and operating system have a set of hard-code certificate authorities and their respective gablic keys (usually several hundred authoritics)	T. a.l	distan	ارسطك	d ,	. 10 (00	وحد	that	l or	e. c	VW 01	N w N	A	30 850	20	do	IJ	nnt	αf	fert	ath	o.c	h	4	Sø 55	e					
Authenticated key exchange (AKE): provides security against active adversouries - Requires a "root of trust" (certificate authority) — we need some binding between keys and identities Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key pk Alice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature sclene) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate (usually several hundred authorities)																				0,11		NOICE	رو	وص	10.0					
Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phasice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate (usually several hundred authorities)	A	lice -		<u>-</u> 110	She	M S	ηστ	م	wbu.	Mi JR	500	CU X	y o	π .	תווכפ		- 1	ممر												
Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phasice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate (usually several hundred authorities)																												\dashv	_	
Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phasice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate (usually several hundred authorities)	Authen	ficocted	Ka	y ex	chang	ze (AKI	E):	provi	ides	وور	usity	oga	inst	ωd	ive	adve	પક્ઝ	شوح									_		
Alice, phase CA (one-time setup, at least for duration of validity period) the certificate binds Alice's public key phasice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature on certificate (usually several hundred authorities)	- þ	Lequires	٥	່ " ເອ	ot e	of tr	ust"	(certi	ficate	out	horit	y)	_	->	we	need	80 M	e l	indir	n k	etwe	en J	ब्रु	an	d <u>id</u>	entitie	<u>s</u>		
the certificate binds Alice's public key pk Alice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scleme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on destriction (usually several hundred authorities)				1																				'						
the certificate binds Alice's public key pk Alice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scleme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on destriction (usually several hundred authorities)			Alice	, PKAL	*				(04	o - fi -	me a	۰.۴۰	Lo.	اما	ايد		ارج،		. 2	ى: ل :اس	., -	المخره	1							
the certificate binds Alice's public key pk Alice to Alice's identity - Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scleme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on destriction (usually several hundred authorities)			_ce	rtaku	<u>.</u>	CA			,014	_ '''	<u>9</u>	e iug	, ut	KV.	1 ۱۵	OF .		ייסיר	U\ \	MIGH	7 T	C, 100	\ J					\top		
- Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature acceptance continuated authorities and their respective gablic keys (usually several hundred authorities)			1		-	_		4																						
- Certificates typically have the following format (X509): - Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - CA's signature acceptance continuated authorities and their respective gablic keys (usually several hundred authorities)			L	4	و دو	stifica:	te	pinds	A	lice's	pabl	ic	Key	PKF	Hice	€	Alice	es 'i	denti	ሃ										
Subject (entity being authenticated) - Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - certificate authorities and their sespective public keys (usually several hundred authorities)	- ر	ertificat																										_		
- Public key (public key for subject for signature scheme) - CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate - CA's signature on certificate - certificate authorities and their respective public keys (usually several hundred authorities)					- 1																									
- CA: identity of the CA issuing the certificate - Validity dates for certificate - CA's signature on certificate			-		. '						Siano	gure	مزجى	me,	١															
- Validity chates for certificate - CA's signature on certificate					•																									
- CA's signature on certificate ————————————————————————————————————) '		34 111																			
certificate authorities and their respective public lays (usually several hundred authorities)												,			.1									,						
(usually several hundred authorities)		- CA	s s	gn actu	ne_	01	ser tit	ficat	೬			<			the.	p10	المكاول	O _r A	d d	per (gnitx O	SYS	Hem	Von	و (S	et c	ते)	narel -	coded
(usually several hundred authorities)															cert	ifica	te o	utho	<i>ાં</i> તાં લ ે	، م	nd "	their	1€	pecti	ive	qabhi	: u	eys .		
																							•			`				
																								ე ე						
																	7	•	1	11 41-1			.,,,							
																												-		
																												_	_	
																												_	_	
																												\rightarrow		
																												+	+	
																												_	_	