TLS 1.3 and authenticated key-exchange quotocols on the Internet typically provide <u>one-sided</u> authentication (i.e., client learns id of the server, but not vice versa)

Question: how does the client authenticate to the server (without providing a certificate) > e.g., how does client login to a web service?

Typical setting: Client and server assumed to have [e.g., client has a password and server] (sk) (sk) client AKE protocol client karns... Server's identification protocol (uk) becomes vulnerable to a man-in-the-middle attack

Threat models: Adversory's goal is to authenticate to server

- Direct attack: advectory only sees vils and needs to authenticate

(e.g., physical analogy: door lock - adversary can observe the lock, does not see the key sk)

- Easses drapping attack: adversary gets to observe multiple interactions between honest client and the server

(e.g., physical analogy: wireless car key - adversory observes communication between car key and car) - <u>Active attack</u>: adversary can impersonate the server and interact with the honest client

(e.g., physical analogy: fake ATM in the mall - honest clients interact directly with the adversary)

Simple (insecure) password-based protocol:

accept if vk= pwd

Not secure even against direct attacks! Adversary who learns vk can authenticate as the client [adversary who breaks into server] [karns user's password!

NEVER STORE PASSWORDS IN THE CLEAR!

Slightly better solution: hash the possibility before storing server maintains mappings Alice \mapsto H(pudAlice) Bob \mapsto H(pudAlice) Where H is a collision-resistant hash function

> <u>client</u> [sk: pud] ______ server [vk: H(pud)]______ _____ pud ______

> > accept if VK = H(pwd)

If passwa														-				
1 1 1	rds have hi	igh entro	ey, then	hard	to re	cover 1	pwd	from I	t(pwd)) [i	by one	- wayne:	5s <i>व</i> र्ग	нJ				
	t not true i																	
Users oft	en choose w	eak pass	iwords ((e.g., 1	23486,	passion	d, 123	345678	9,)									
	n a dictiona										nouseo	U)	Base	id on	passes	und has	ites that	have
	(3% choose	123456)								1		1		been	, leake	ed from	r compe	omised
	(10% choose	amona to	e 25 cm	mman ma	الالالاللال)						J	1	dato	<i>bases</i>			
Suda hali		, ttt	diction		, ahr													
	ing vulnerable								_	· · ·	664							_
	vey computes																	
	H(pud), can						0.											
	for Linked In	breach in	2012, a	ittacker	stole	possword	file	with	~6 m	illion a	محصم	(1 6)						
	(all passions	rds hasted	h using	single it	remotion	of uns	alted	SHA-1) —	-> 90	% of	possivo	nds r	ecorre	d in	~ 6	days!	
Problem: 0.	ne-time prec		• T															
		cost of		-												ot p	strucerc	to a
Defense #1	: Salt on a	words to	efore has	hina:	namelu	when s	toring	00.564	rg er	Nd	Samolo	5	ut e	- 20.1	3	and	store	
	: <u>Salt</u> poss														۲ ۲			
						-((salt)) rr.			-10L 1	JC3 (764		_		+	ypically,	, n ≥ (64	
	<u>Note</u> : Sa	art is a	public vo	nne (n	used -	tor venti	cation)			+				\vdash	<u>r / </u>			
																		+
Offline	dictionary at	tack no	longer e	effective	. Eince	every	Salt	value	induces	s deffe	rent s	set of	has	h value	ى			
		cost of																
	: Use a g																	
	- PBKD	FJ (pass	scoord -bas	ed key	-derive	tion fun	iction)	: teroi	te a	crypton	graphic	hash	func	tion n honest	nany ruser	times: only ru	eeds to	eratur
	- PBKD		scoord -bas	ed key	-derive	tion fun H(H(·	uction) ····H(salt 119	te a wd) ···	crypto; .))	graphic	hash	func	honest	r user	only ne	eeds to ce per	esolue auther
	- PBKD	FJ (pass	scoord -bas	ed key	-derive	tion fun H(H(·	uction) ····H(salt 119	te a wd) ···	crypto; .))	graphic	hash	func	honest hash	t user functi	only ne ian Onc	ce per	auther
	- PBKD (or ber)FJ (pass Ypt)	rusard -bas PBKDFö	sed key 2 (pud,	-derivion salt):	thion fur H (H(· Cau	n use	: 'teroi salt 9 100,00 (,000,0	te a wd) 0 or 000 ite	crypter)) crostions	graphic	hash	func	honest hash	t user functi	only ne ian Onc	eeds to ce per tes <u>ma</u>	auther
	- PBKD (or ber <u>Dr</u>)FJ (pass rypt) <u>ausback</u> : cr	usord -bas PBKDFd Ustom ha	ed key 2 (pud, odware	-derivion solt): con es	trion fun H (H(· Cou soluate	uction) H(In use SHA-2	interse solt 11 g 100,00 (,000,0 256 <u>v</u>	te a wh) 0 or 000 ite ery fi	crypton)) crostions fast	graphic of SHI	hash 19-256	func	honest hash adver	t user Functi Boxy	only ne ian Onc Qsaluet	ce per tes <u>ma</u>	auther
	- PBKD (or bea <u>Dr</u> - Scryp)FJ (pass rypt) r <u>awback</u> : ci t (more e	usord -bas PBKDF6 ustom ha recent : A	sed key 2 (puid, rohusere trojon 2:i)	-deriver salt): can ev ; slow	tion fun H(H(· Cou soluote s hash	uction) H(n use SHA-2 functi	: there solt 9 100,00 (,000,00 (,000,0 256 <u>v</u> ion th	te a wh) o or oos ite ecy fi at ru	crypton)) erostions ast eeds	of SHI lots e	. hash 1236 өf <u>ma</u>	tune	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	auther
	- PBKD (or ber <u>Dr</u> - Scryp)F2 (pass rypt) <u>ausback</u> : cu t (more a custom b	usord-bas PBKDFö ustom hou recent: A nardusare	sed kay 2 (puid, rdware tryon 2:) do not	-derive salt): can ev ; slow provid	tion fun H(H(- Cas Saluate a Saluate a Saluate a	ction) H(N USE SHA-2 Functi tranhal	: iteroi (sult p 100,00,00 (,000,00 (,000,00 (,000,00 (,000,00 (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00) (,000,00)	te a wh) o or soo ite ery fi at ru as (1	crypton)) prostions ast eeds liniting	graphic of SHI lots e facte	hash A-256 of <u>ma</u>	tune	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	auther
	- PBKD (or ber <u>Dr</u> Scryp L> Can albo)FJ (pass rypt) <u>ausback</u> : cu t (more e custom b Use a	usord-bas PBKDF6 usotom hav recent: f hardware <u>keyed</u>	sed key 2 (psd, rdware tryon 2:) do not hash fi	-derive salt): can ev : slow pravið hunction	tion fun H (H(· Cou Boluote S hash (e.g., 1	ction) H H H H H H H H H H H H H	: the noise sould be a first f	the a wh) o or poor ite eny fi at nu bay hey	crypton)) prostions ast eeds linuiting stored	of SHI lots o facto in h	. hash 19-256 5f <u>me</u> 5r is 15M)	func	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	Quethere
	- PBKD (or ber <u>Dr</u> Scryp L> Can albo)F2 (pass rypt) <u>ausback</u> : cu t (more a custom b	usord-bas PBKDF6 usotom hav recent: f hardware <u>keyed</u>	sed key 2 (psd, rdware tryon 2:) do not hash fi	-derive salt): can ev : slow pravið hunction	tion fun H (H(· Cou Boluote S hash (e.g., 1	ction) H H H H H H H H H H H H H	: the noise sould be a first f	the a wh) o or poor ite eny fi at nu bay hey	crypton)) prostions ast eeds linuiting stored	of SHI lots o facto in h	. hash 19-256 5f <u>me</u> 5r is 15M)	func	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	Quethere
	- PBKD (or ber <u>Dr</u> Scryp L> Can albo)FJ (pass rypt) <u>ausback</u> : cu t (more e custom b Use a	usord-bas PBKDF6 usotom hav recent: f hardware <u>keyed</u>	sed key 2 (psd, rdware tryon 2:) do not hash fi	-derive salt): can ev : slow pravið hunction	tion fun H (H(· Cou Boluote S hash (e.g., 1	ction) H H H H H H H H H H H H H	: the noise sould be a first f	the a wh) o or poor ite eny fi at nu bay hey	crypton)) prostions ast eeds linuiting stored	of SHI lots o facto in h	. hash 19-256 5f <u>me</u> 5r is 15M)	func	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	Quethere
Best practic	- PBKD (or bea <u>Dr</u> - Scryp L> Can albo L>	F2 (pass rypt) <u>ausback</u> : ci t (more e custom t Use a ensures	usord -bas PBKDF6 usotom ha recent : f hardware <u>keyed</u> adversary	sed key 2 (psd, rdware tryon 2:) do not hash fi	-derive salt): can ev : slow pravið hunction	tion fun H (H(· Cou Boluote S hash (e.g., 1	ction) H H H H H H H H H H H H H	: the noise sould be a first f	the a wh) o or poor ite eny fi at nu bay hey	crypton)) prostions ast eeds linuiting stored	of SHI lots o facto in h	. hash 19-256 5f <u>me</u> 5r is 15M)	func	honest hash adver (space	t user functi Eory e) te	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	Quethere
Best proction	- PBKD (or ber <u>Dr</u> Scryp Can albo L> <u>ce</u> : Alwoys	F2 (pass rypt) ausback: cu t (more e custom t use a ensures solt passe	usord -bas PBKDFd usotom hav recent : f hardware <u>keyed</u> adversary	sed key 2 (psd, rdwsore trojon 2:) do not hash fi who a	-derive salt): can ev : slow pravið hunchion dæs no	tion fun H (H(. Cou Boluote S hash Ne subor (e.g., 1 ot know	iction) H H H H H H H H H H H H H	: Herod solt 9 100,00 (000,00 256 <u>v</u> ion th sastin (with Canno	te a wh) o or poo ite eny fi at rv hey hey t br	crypton)) crostions ast eeds linnihimy stored whe fo	of SHI lots c facts in h	. hosh A-256 of <u>ma</u> or is HSM) HSM)	func (<u>space</u>	horest hash adver (space e, Aot	t user functi Bory <u>e</u>) te comp	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	Quethere
Best proctic	- PBKD (or ber <u>Dr</u> Scryp Can albo L> <u>ce</u> : Alwoys	F2 (pass rypt) <u>ausback</u> : ci t (more e custom t Use a ensures	usord -bas PBKDFd usotom hav recent : f hardware <u>keyed</u> adversary	sed key 2 (psd, rdwsore trojon 2:) do not hash fi who a	-derive salt): can ev : slow pravið hunchion dæs no	tion fun H (H(. Cou Boluote S hash Ne subor (e.g., 1 ot know	iction) H H H H H H H H H H H H H	: Herod solt 9 100,00 (000,00 256 <u>v</u> ion th sastin (with Canno	te a wh) o or poo ite eny fi at rv hey hey t br	crypton)) crostions ast eeds linnihimy stored whe fo	of SHI lots c facts in h	. hosh A-256 of <u>ma</u> or is HSM) HSM)	func (<u>space</u>	horest hash adver (space e, Aot	t user functi Bory <u>e</u>) te comp	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	auther
Best proctic	- PBKD (or been Dr - Scryp- L> Can also L> ce: Always Always	F2 (pass ypt) ausback: cu t (more t custom t use a ensures solt passo use a s/	usord -bas PBKDFd usotom hav recent : A randware kayed adversary words bas hash	sed key 2 (psd, rdware troon 2:1) do not hosh fi who a function	-derive salt): can ev : slow pravið hunchion dæs no	tion fun H (H(. Cou Boluote S hash Ne subor (e.g., 1 ot know	iction) H H H H H H H H H H H H H	: Herod solt 9 100,00 (000,00 256 <u>v</u> ion th sastin (with Canno	te a wh) o or poo ite eny fi at rv hey hey t br	crypton)) crostions ast eeds linnihimy stored whe fo	of SHI lots c facts in h	. hosh A-256 of <u>ma</u> or is HSM) HSM)	func (<u>space</u>	horest hash adver (space e, not	t user functi Bory <u>e</u>) te comp	only ne ian Onc Oschud o essalu	ce per tes <u>ma</u>	auther
Best proctic	- PBKD (or bee Dr - Scryp L> Can albo L> ce: Alwoys Alwoys SCI	F2 (pass ypt) <u>ausback</u> : cr t (more e custom t use a ensures solt pass use a s/ use a s/	Histord -bas PBKDFd Ustom hav recent : A hardware keyed adversory words bas hash	sed key 2 (psd, 1900 2:1) do not hash fi who function	-derive salt): salt): slow provid hunction does no	tion fun H (H(. Cou soluate s hash le subor (e.g., 1 st know g., PBKD	n use SHA-2 functi tuntal HMAC bey	: Herod Sould II 9 100,00 100,00 256 <u>v</u> 256 <u>v</u> ion the Source Connec Connec Connec	te a wh) o or ite ery fi at ru hey t br or	crypton)) crostions ast eeds linnihimy stored whe fo	of SHI lots c facts in h	. hosh A-256 of <u>ma</u> or is HSM) HSM)	funce (space	horest hash adver (<u>space</u> e, not	t user functi sory e) te comps	only ne (an Onc essalue e essalu ste)	se per tes <u>ma</u> nate	auther
Best proctic	- PBKD (or bee <u>Dr</u> - Scryp L> Can also L> ce: Always Always SCI \$CI	F2 (poss ypt) <u>ousback</u> : cr t (more t custom t use a solt posse use a st use a st ur = 'p ur = m	PBKDFd PBKDFd ustom hav recent : A randware kayed adversary words bus hash	sed key 2 (pood, 10gon 2:1) do not hosh fi who function Drd' Ur) m	-derive salt): salt): slow pravid unction does no (en	tion fun H (H(- Cou soluate soluate soluate soluate (e.g., 1 ot know g., PBKD soluate soluate (e.g., 1 soluate (e.g., 1) soluate (e.g.,	ction) H H H H H H H H H H H H H	: the nois solt 11 9 100,00 1,000,00 256 <u>v</u> ion the source conno conno crypt) secure	the a wh) o or poor ite eny fi at ru bay t br or ()	crypton)) crotions cast eeds stored stored whe fo keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	func (space I I Face	horest hash adver (space e, not	t user functi socy <u>e)</u> te comps h!	only ne ian Onc essalues e essalu ste)	se per tes <u>ma</u> note	aucther
Best procti	- PBKD (or bee <u>Dr</u> - Scryp L> Can also L> ce: Always Always SCI \$CI	F2 (poss ypt) <u>ousback</u> : cr t (more t custom t use a solt posse use a st use a st ur = 'p ur = m	PBKDFd PBKDFd ustom hav recent : A randware kayed adversary words bus hash	sed key 2 (pood, 10gon 2:1) do not hosh fi who function Drd' Ur) m	-derive salt): salt): slow pravid unction does no (en	tion fun H (H(- Cou soluate soluate soluate soluate (e.g., 1 ot know g., PBKD soluate soluate (e.g., 1 soluate (e.g., 1) soluate (e.g., 1	ction) H H H H H H H H H H H H H	: the nois solt 11 9 100,00 1,000,00 256 <u>v</u> ion the source conno conno crypt) secure	the a wh) o or poor ite eny fi at ru bay t br or ()	crypton)) crotions cast eeds stored stored whe fo keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	func (space I I Face	horest hash adver (space e, not	t user functi socy <u>e)</u> te comps h!	only ne (an Onc essalue e essalu ste)	se per tes <u>ma</u> note	aucther
Best proctiv	- PBKD (or bea - Scryp- L> Can also L> Can also L> Can also L> Scryp- Can also L> Can Also L Can Also L C Can Also L C Can Also L Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C C Can Also L C C C C C C C C C C C C C C C C C C	F2 (poss ypt) <u>ousback</u> : cr t (more to crustom to use a solt posse use a st use a st ur = 'p ur = m alt = ra ur = hi	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF	sed key 2 (pood, hogen 2:1) do not hosh fi whe function prd' ur) ru es(20 ha1(!	-derive salt): salt): salt): slow pravid unction does no does no (en (en ava MD)) \$CUr,	tion fun H (H(- Cou soluate soluate soluate soluate (e.g., 1 ot know g., PBKD solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution	ction) H H H H H H H H H H H H H	in the with solt II g 100,00 100,00 256 <u>v</u> ion th source with Conno crypt) secure	te a which ite o or oon ite ent ru bay t br or () t bay t br or () t bay	crypton)) crotions ast eeds limiting stored whe fo keyed keyed keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	func (unory space in Fac =)	- honest hash adver (<u>space</u> e, not r <u>both</u> ebook	t user functi socij e) te compu h! posti	only ne ian Onc essalues > essalu > essalu > essalu > essalu > essalu > > essalu > > > > + + + + + > > + + + + + + + +	re per tes <u>ma</u> note	
Best proctiv	- PBKD (or bea - Scryp- L> Can also L> Can also L> Can also L> Scryp- Can also L> Can Also L Can Also L C Can Also L C Can Also L Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C Can Also L C C Can Also L C C C C C C C C C C C C C C C C C C	F2 (poss ypt) <u>ousback</u> : cr t (more t custom t use a solt posse use a st use a st ur = 'p ur = m	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF	sed key 2 (pood, hogen 2:1) do not hosh fi whe function prd' ur) ru es(20 ha1(!	-derive salt): salt): salt): slow pravid unction does no does no (en (en ava MD)) \$CUr,	tion fun H (H(- Cou soluate soluate soluate soluate (e.g., 1 ot know g., PBKD solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution Solution	ction) H H H H H H H H H H H H H	in the with solt II g 100,00 100,00 256 <u>v</u> ion th source with Conno crypt) secure	te a which ite o or oon ite ent fi at ru bay t br or () t bay t br or () t bay	crypton)) crotions ast eeds limiting stored whe fo keyed keyed keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	func (unory space in Fac =)	- honest hash adver (<u>space</u> e, not r <u>both</u> ebook	t user functi socij e) te compu h! posti	only ne ian Onc essalues > essalu > essalu > essalu > essalu > essalu > > essalu > > > > + + + + + > > + + + + + + + +	se per tes <u>ma</u> note	
Best procti	- PBKD (or bee Dr - Scryp Can albo L> Can albo	F2 (poss ypt) <u>ousback</u> : cr t (more to crustom to use a solt posse use a st use a st ur = 'p ur = m alt = ra ur = hi	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF	ed key 2 (pood, do not hosh fi who function ord' ur) ra es(20 ha1(!	-derive salt): salt): salt): slow provid does no does no does no does no does no does no does no does no	tion fun H (H(- Cou soluate b hash le subor (e.g., 1 ot know g., PBKD S hash - \$salt 1a256	ction) H H H H H H H H H H H H H	solt II g 100,00 100,00 256 <u>v</u> 256 <u>v</u> 257	te a wh) 0 or 1000 ite ery fi at ru heay t br or ited, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted	crypton)) crotions ast eeds limiting stored whe fo keyed keyed keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	funce funcery space I I Face age	honest hash adver (<u>space</u> e, Aot e, Aot esbook ((ers gr	t user functi sory e) te comps h! passes comps	only ne (an Onc essalue = essalue =	re per tes <u>ma</u> note	courthear
	- PBKD (or bea - Scryp- - Scry	F2 (poss ppt) <u>ausback</u> : cr t (more a custom t use a ensures solt passe use a sl ur = 'p ur = m alt = ra ur = hi ur = re	PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF PBKDF	ed key 2 (pod, 2 (pod, 2 (pod, 2 (pod, 1) do not hosh fi who function prd' ur) ra es(20 ha1(s ha1(s	-derive salt): salt): salt): pravid unction does no does no (en (en (en scur, ac_sh \$salt	tion fun H (H(. Cou Boluote S hash (e.g., 1 ot know g., PBKD S hash- \$salt 1a256) slo	ction) H(In use SHA-2 function transtantion HMAC bey DF2, set 	solt II g 100,00 100,00 256 <u>v</u> 256 <u>v</u> 257	te a wh) 0 or 1000 ite ery fi at ru heay t br or ited, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted, iculted	crypton)) crotions ast eeds limiting stored whe fo keyed keyed keyed	of SHI lots c facto in h stree <u>a</u> hash	hosh A-256 of <u>me</u> or is HSM) HSM) Hancht	func (space ! ! Fac :) lay	horest hash adver (<u>Epace</u> e, Not e, Not ebook (ers ge achieve	t user functi socy e) te comps f. f. passe icirca raduall e bet	only ne ian Onc essalues e essalues ute) ute) Jacolity Her s	se per tes <u>ma</u> nate nion)	eurther <u>ay</u> ti

Password-based protocol not secure against eavesdropping adversory

(adversary sees vic and transcript of multiple interactions between honest prover + honest verifies)

One-time passwords (SecurID tokens, Google authenticator, Duo) (OTP) Construction 1: Consider setting where verification key VK is secret (e.g., server has a secret) - Client and server have a shared PRF key to and a counter (initialized to 0): client (k, c) $c', y' \in F(k, c)$ f $c \in C+1$ $concretely: con integret if successful, update <math>c \leq c'$ $c \in C+1$ $concretely: con integret if successful, update <math>c \leq c'$ output as 6-digit Num ber - <u>RSA SecurID</u>: stateful token (counter incremented by pressing button on token) > State is cumbersome - need to maintain consistency between client/server - Google Authenticator: time-based OTP: counter replaced by current time windows (e.g., 30-second windows) If PRF is secure => above protocol secure acquires eaves droppers (but requires server secrets) Lo can be problematic : RSA breached Construction 2: No server-side secrets (3/Key) under composition in 2011 and SecurID tokens companies - Relies on a hash function (should be one-way) and used to compromise detense - Secret key is random input x and counter n; Contractor Lockheed Martin Verification key is $H^{(n)}(x) = H(H(\dots H(x)\dots))$ n evaluations of H pudn pudn-1 pudz pudz to verify y: check $H(y)^{\frac{1}{2}} vk$ (attacker has to invest H J in order to authenticate if successful, update vk < y x $H(x_1 H_{(y_2)}(x_1) H_{(y_{-2})}(x_1) H_{(y_{-1})}(x_1) H_{(y_1)}(x_1 = h)^{n}$ - Verification key can be public (credential is preimage of UK) L=> Can support bounded number of authentications (at most n) - need to update key after n logins L> Output needs to be large (~80 bits or 128 bits) since password is the input /output to the hash function - Natively, client has to evaluate H many times per authentication (20(1) times) L> Can reduce to O(log n) hash evaluations in an omortized sense by storing O(log n) entries along the hash chain Thus for, only considered possive adversories, but in reality, adversaries can be <u>malicious</u> no man-in-the-middle

- Advectory can impersonate server (e.g., phishing) and then try to authenticate as client (but cannot interact with client during anth.) - All protocols thus for are valuerable [all consist of client sending taken that server checks, which can be extracted by] active adversory

- For active security, we use <u>challenge-response</u>