lecture 19

$\boxed{\text{Digital Signatures}}$

DS from reversible public-key Encryption.

$\boxed{\text{PkE\_reversible}}$: suppose E_e is a public-key Enc scheme with message space "$\mathcal{M}$" & cipher space "C", let $\underline{\mathcal{M} = C}$.

suppose D_d : d is the private key.

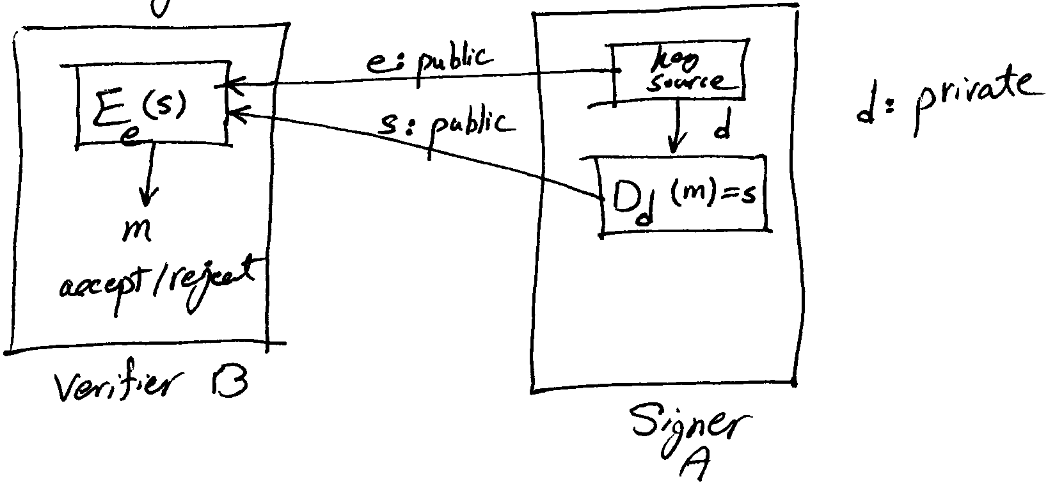
$$D_d(E_e(m)) = E_e(D_d(m)) = m \quad \text{for all } m \in \mathcal{M}$$

this is not "ciphertext"

★ Constructon of a simple digital signature scheme

1. Let $\mathcal{M}$ is message space
2. Let $\mathcal{M} = C$, C is the signature space.
3. let (e,d) be a pair key of scheme
4. signing Function S_A is $D_d \longrightarrow \underset{\text{signature}}{s} = D_d(m)$
5. verification Function V_A :

$$V_A(\underset{\text{message}}{m}, \underset{\text{signature}}{s}) = \begin{cases} \text{'true'} & \text{if } E_e(s) \overset{=m}{\in} \mathcal{M} \\ \text{'false'} & \text{otherwise} \end{cases}$$



requirmets:

- It must be easy to compute by signer
- It must be easy to verify by verifier
- Have an appropriate lifespan → be computationally secure from forgery

Resolution of disputes:

For example: "A" could at some point <u>deny</u> having signed a message or other entity "B" could falsely <u>claim</u> that a signature on a message was produced by entity "A".

Basic Definitions

- Digital Signature: it's a data string which associates a message (in digital form) with some originating entity.
- A digital signature generation alg. is a method for producing a digital signature.
- A digital signature verification algo. is a method for verifying that a digital signature is <u>authentic</u>.
- DS scheme → DS gen alg.
  DS scheme → DS ver alg.

DS schemes → DS schems with <u>appendix</u>: requre the original message as input to the verification algorithm.

DS schemes → DS schemes with <u>message recovery</u>: do n't require the original message as input to ver alg. → original message is recoverd from the signature

① (message) "$\mathcal{M}$" is the set of elemets to which a signer can affix a digital signature.

② (signing space) "$\mathcal{M}_S$" is the set of elemets to which the signature transformations are applied.

Note: the signature transformations are not applied directly to "$\mathcal{M}$"

③ (signature space) "S" is the set of elemets associate with message in "$\mathcal{M}$".

purpose: to <u>bind</u> the signer to a message.

④ (indexing set) "$\mathcal{R}$" is used to identify specific signing transformations.

$\boxed{\text{Def DS}}$: A digital signature scheme (with either appendix or message recovery) is said to be a randomized DSS if $|\mathcal{R}| > 1$ (more than one signing transformations); otherwis, the DSS is said to be deterministic.

one-time signature scheme

multiple-use scheme

Alg: signature gen & verification:

Summary: "A" produces a signature "s" $\in$ "S" for a message "$\tilde{m}$" $\in \mathcal{M}$, which can later be verified by "B".

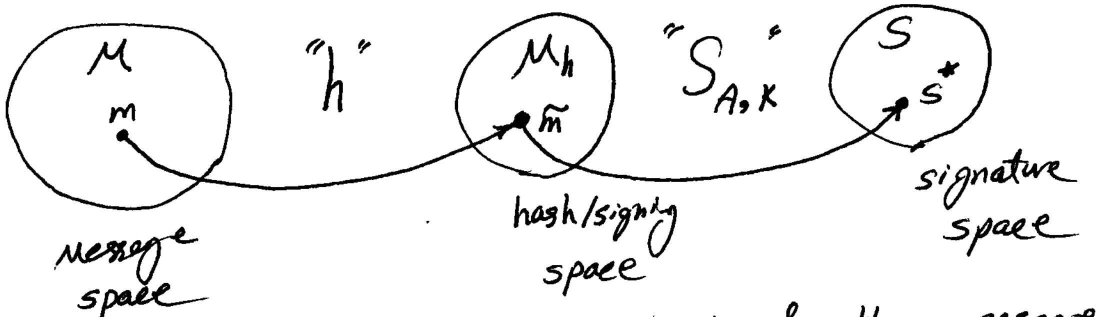
1. signature generation: "A"

1.1: element $k \in \mathcal{R}$ → to select which singing transformation should be used

1.2: Compute $\tilde{m} = h(m)$

$$s^* = S_{A,k}(\tilde{m})$$

1.3: A's signature for "m" is s^*. Both "m" & s^* are made available to "B" for verification.



Note: You must sign the hash of the message NOT the message itself.

Both parties have access to original "message"

External

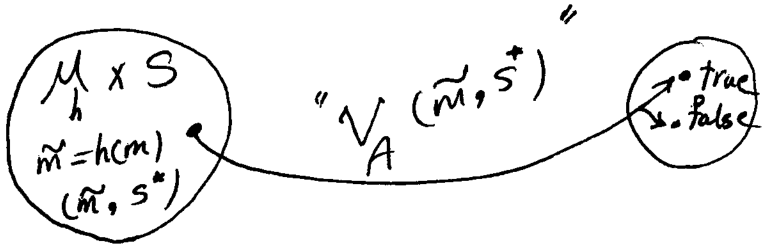
2. verification: "B"

2.1 obtain A's authentic public key V_A

2.2 Compute $\tilde{m} = h(m)$ and $u = V_A(\tilde{m}, s^*)$

2.3 Accept the signature if and only if "u" = true

Note: DSS with message recovery we can use RSA Rabin



Note: S_A : private
V_A : public