CSE 599B Lecture 1

Note Title 1/4/2006

Cryptography

Secret Writing

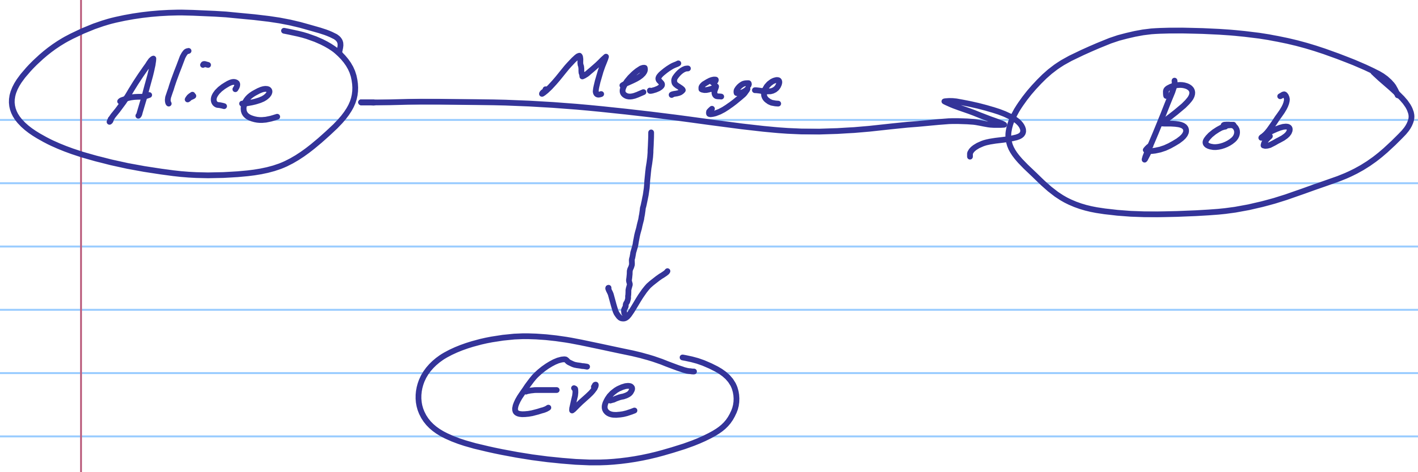
Original Setting:

2(3) parties: Alice / Sender

Bob / Receiver

Eve / Evesdropper

Alice wishes to send to Bob over <u>insecure</u> channel.



Insecurity of channel: Eve

2 types of Eve:

- Passive → Evesdrop
- Active → Can modify what is sent on the channel but cannot sever the channel entirely

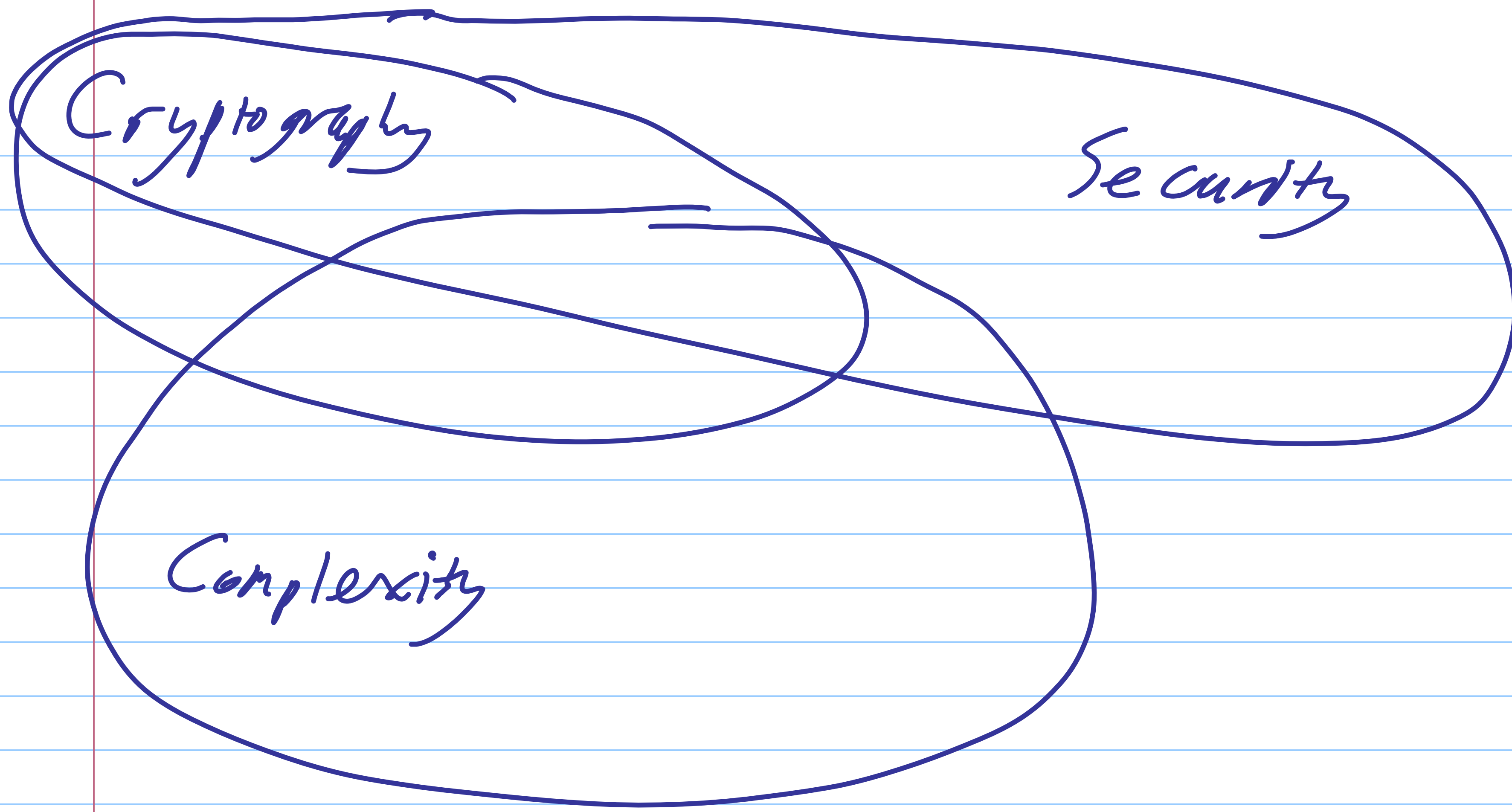
Desiredata:

Secrecy: by observing communication, Eve cannot learn anything about the message that she didn't already know.

Authenticity: The message that Bob receives is the same message M that Alice sent.

Many other scenarios:

- Access control (passwords) / general authentication
- Privacy of data
- Electronic Payments
- Electronic Voting
- Bit commitment
- pseudorandom generators



To get secrecy

Bob must know something Eve does not (Secret Key)
or Bob has a capability Eve does not.

To get Authentication:

Sender must know something Eve does not.
(Secret key)

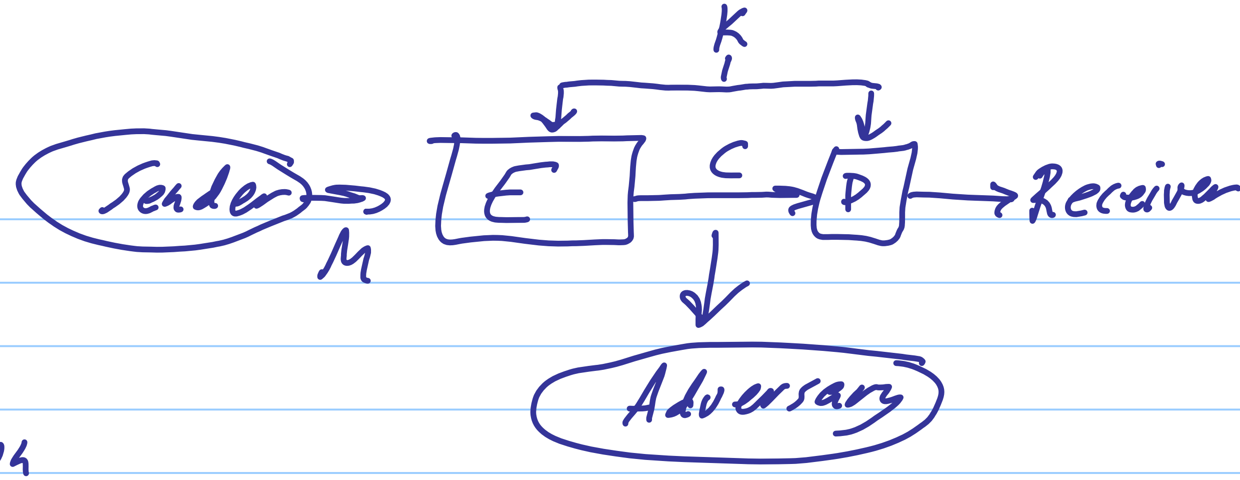
Two scenarios: Trust Models

Symmetric (Shared Key / Private Key) Model:

Alice & Bob share key K

Asymmetric (Public key): Each party has a key.

Symmetric Encryption:



M: Message (plaintext)

C: Cyphertext

3 algorithms

E: encryption

D: decryption

: Key generation

$\mathcal{K}$: set of possible keys

$\mathcal{M}$: space of messages

$\mathcal{C}$: space of ciphertexts

$E: \mathcal{K} \times \mathcal{M} \longrightarrow \mathcal{C}$

$D: \mathcal{K} \times \mathcal{C} \longrightarrow \mathcal{M}$

Sender $C \leftarrow E(K, M) = E_K(M)$

Sends C on channel

Receiver $M \leftarrow D(K, C) = D_K(C)$

Need: $M = D_K(E_K(M))$

typically will leak info about length of M

Choice of key $k \in \mathcal{K}$

Must be random else adversary could predict it.

typically key generation will just be uniform choice over $\mathcal{K}$

eg $\mathcal{K} = \{0, 1\}^*$

$\mathcal{K} = \{ pq \mid p, q \text{ are } n \text{ bit primes} \}$

$k_R \leftarrow \mathcal{K}$ means uniform distribution for k from $\mathcal{K}$

We want security no matter how sender sends

$m \in \mathcal{M}$

Adversary may know m is English text

or 0^n or 1^n

$k = \log |\mathcal{K}|$ security parameter

number of bits to represent

One-time pad

$\mathcal{K} = \{0,1\}^K$

$\mathcal{M} = \{0,1\}^n = \mathcal{C}$

$n \le K$

Key generation:

$K \leftarrow_R \{0,1\}^K$

static counter $\leftarrow 0$

$E_K(M) =$ $C_i \leftarrow M_i \oplus K_i$ for $i = 1$ to n

output C, counter

counter $\leftarrow$ counter $+ n$

$D_K(C) =$ $m_i \leftarrow C_i \oplus K_i$ for $i = 1$ to n

output M

since $M_i = (M_i \oplus K_i) \oplus K_i$

Reusing one the pad:

$$M \to C$$
$$M' \to C'$$

$$C \oplus C' = (M \oplus K) \oplus (M' \oplus K)$$
$$= M \oplus M'$$

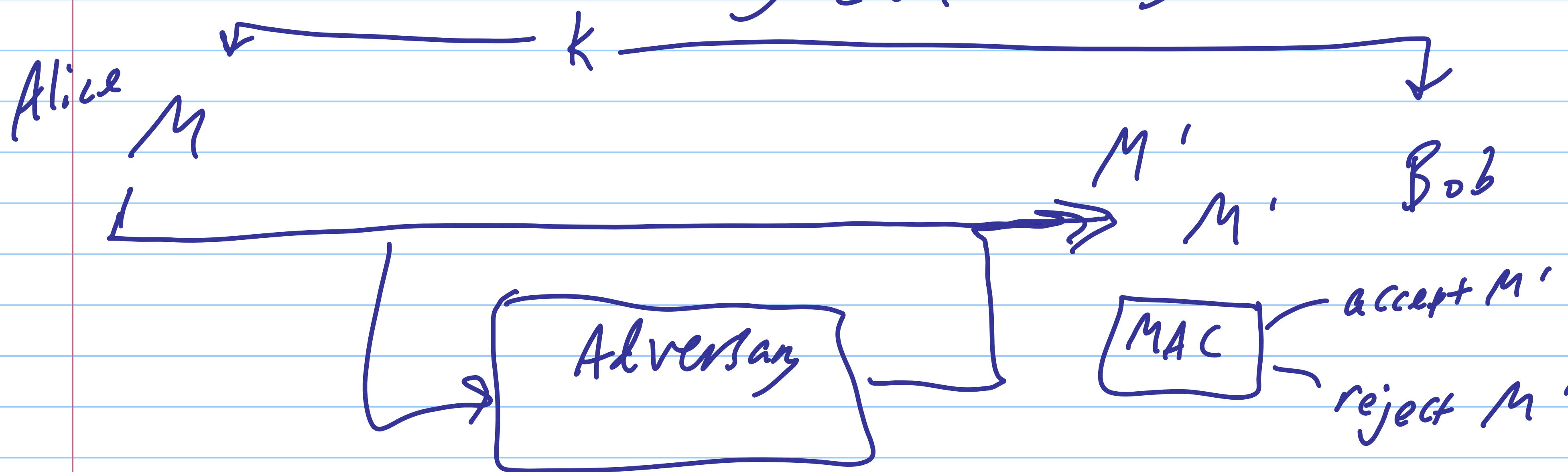
Nova documentary:

Julius Rosenberg (& Ethel) caught sending nuclear secrets to Soviets using a one-time pad

Authentication:

Symmetric: MAC (Message Authentication Code)

tag each message



Sender computes $tag = MAC_k(M)$

sends $\langle M, tag \rangle$

receiver $\langle M', tag' \rangle$

receiver computes $tag'' = MAC_K(M')$

rejects iff $tag' \neq tag''$

Adversary should not be able to convince receiver tag' is valid for changed message M'

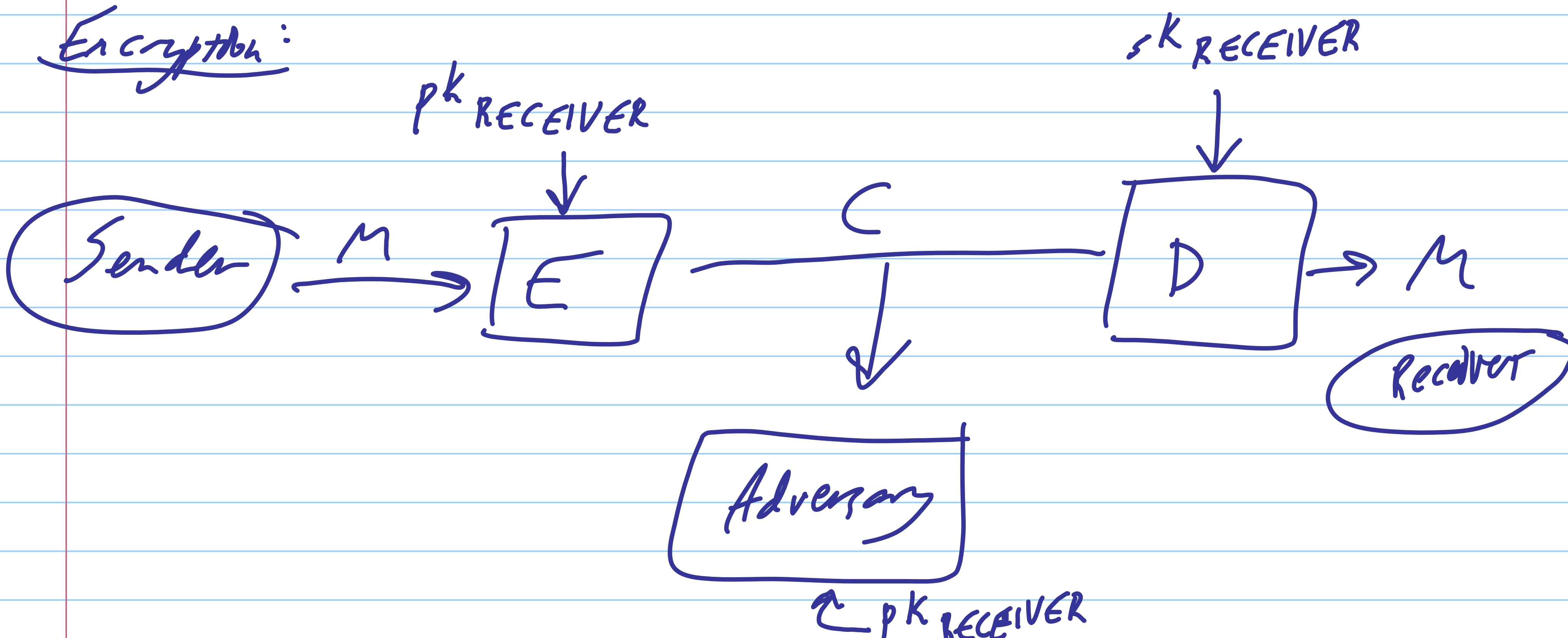
Asymmetric encryption: (Public Key Encryption)

Two keys for each party A

public key: pk_A

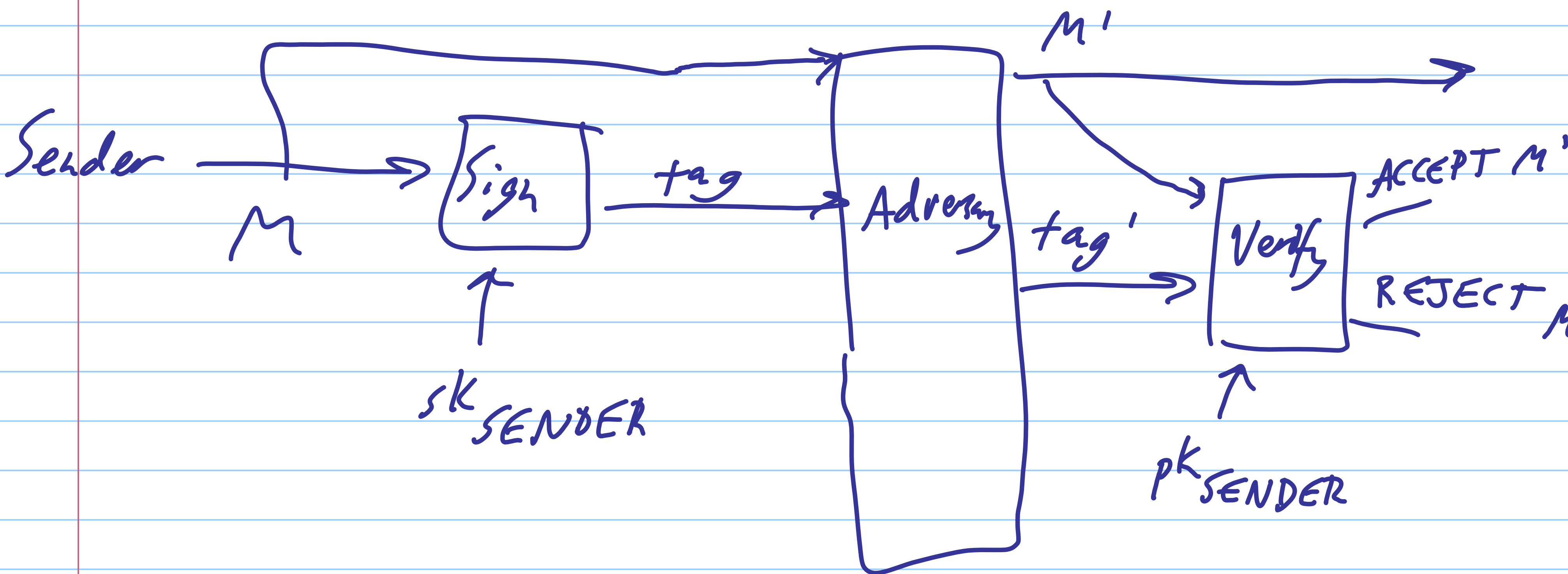
secret key: sk_A

Encryption:



Authentication:

Digital Signatures (public key version of MAC)



	private symmetric	public Asymmetric
Secrecy		
authentication		

Shannon (1949)

Security

Definition: Symmetric Encryption Scheme secure iff for all distributions m

$$\Pr_{m,k}[M \mid C = E_k(M)] = \Pr_m[M]$$

Theorem (Shannon 1949) If symmetric encryption is perfectly secure, then $|M| \le |K|$

Theorem for $n \leq k$ One-time pad is perfectly secure.

$$\Pr_{k,m}[C \mid M] = \Pr_{k,m}[C]$$