CS155a: E-Commerce

Lecture 6: Sept. 25, 2001

Technical-Protection Services for Online Content Distribution

Symmetric-Key Crypto

$D(E(x, k), k) = x$

(decryption, encryption, plaintext, key)

- Alice and Bob choose k_{AB}
- Alice: y <-- $E(x, k_{AB})$ (ciphertext)
- Alice --> Bob: y
- Bob: x <-- $D(y, k_{AB})$

(Eve does not know k_{AB})

Well Studied and Commercially Available

- DES
- IDEA
- FEAL-n
- RC5

✸AES

Users must deal with key management

Public-Key Crypto

$D(E(x, PK_u), SK_u) = x$

(user's Secret Key, user's public key)

Bob generates SK_{bob}, PK_{bob}

Bob publishes PK_{bob}

Alice: Lookup PK_{bob}

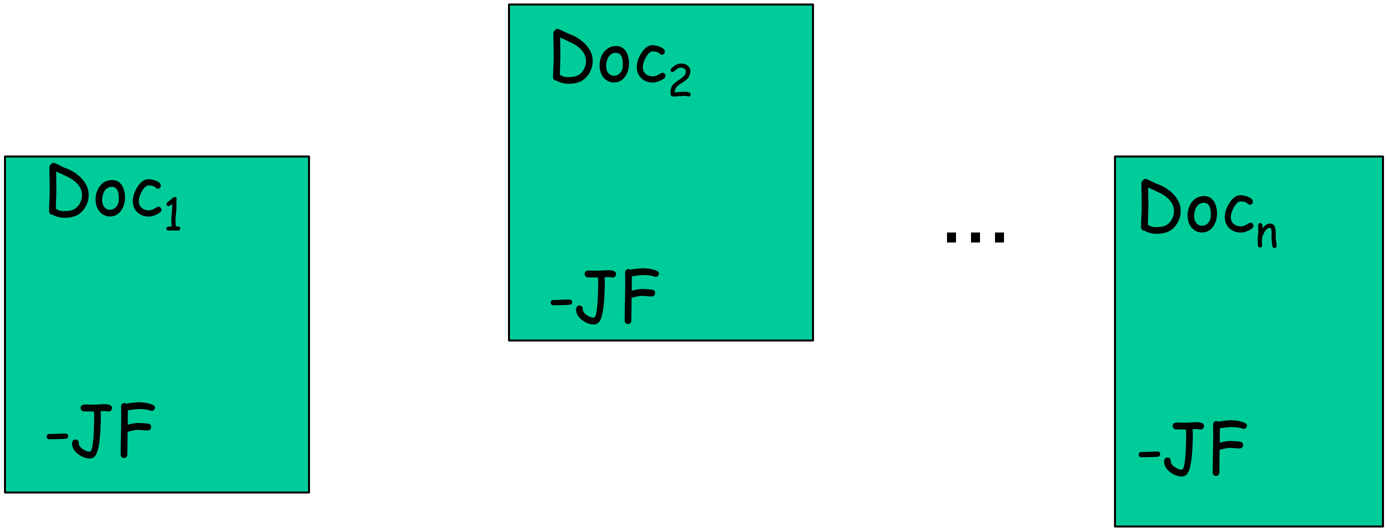
y <-- $E(x, PK_{bob})$

Alice -->Bob: y

Bob: x <-- $D(y, SK_{bob})$

(Eve does not know $SK_{bob.}$)

Digital Signatures



Doc$_1$

-JF

Doc$_2$

-JF

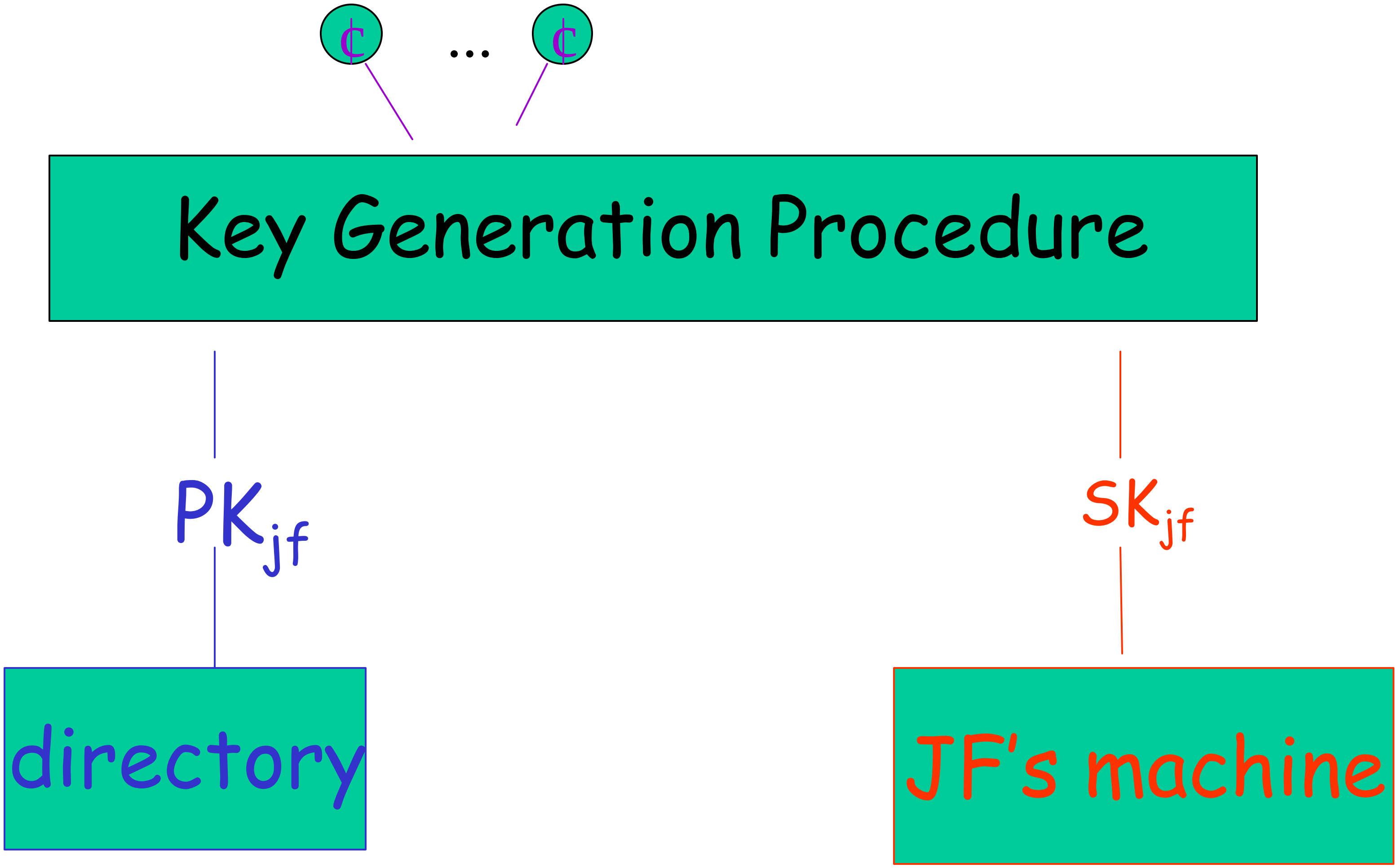
…

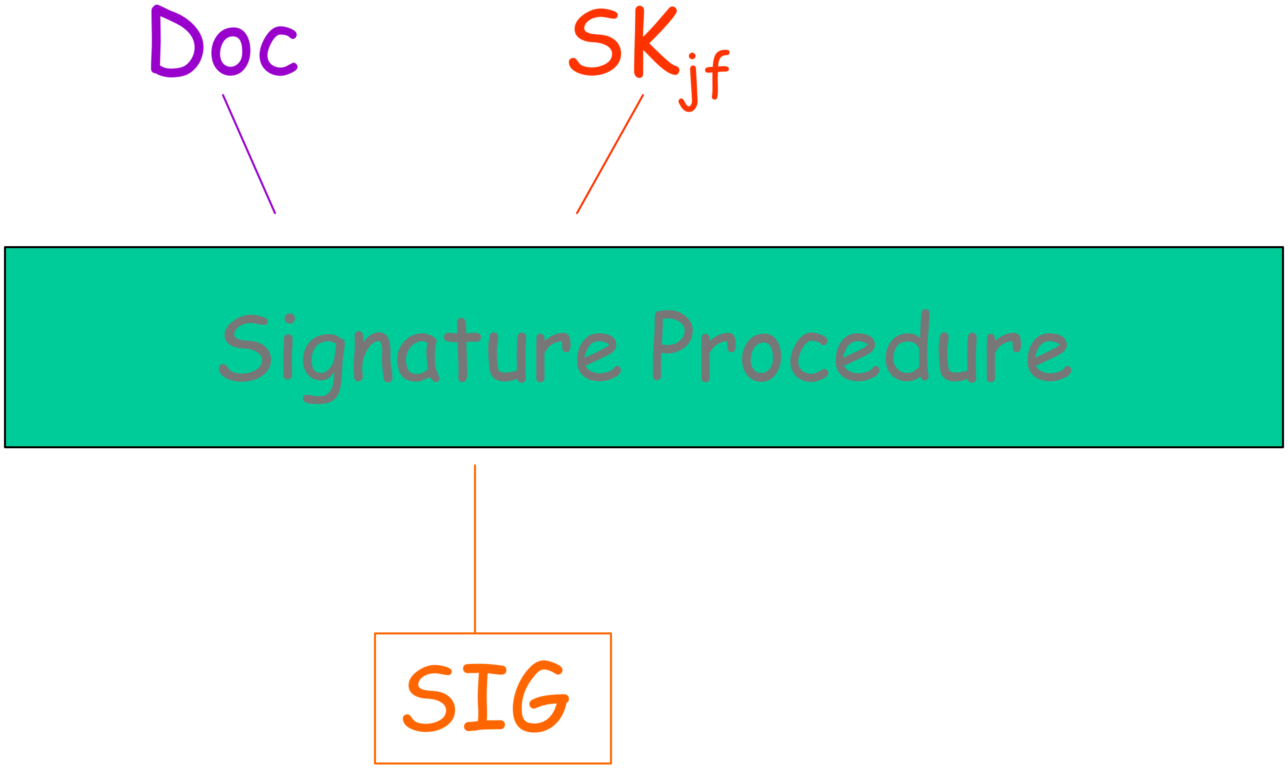
Doc$_n$

-JF

Trickier than the paper "analogue"

3-part Scheme



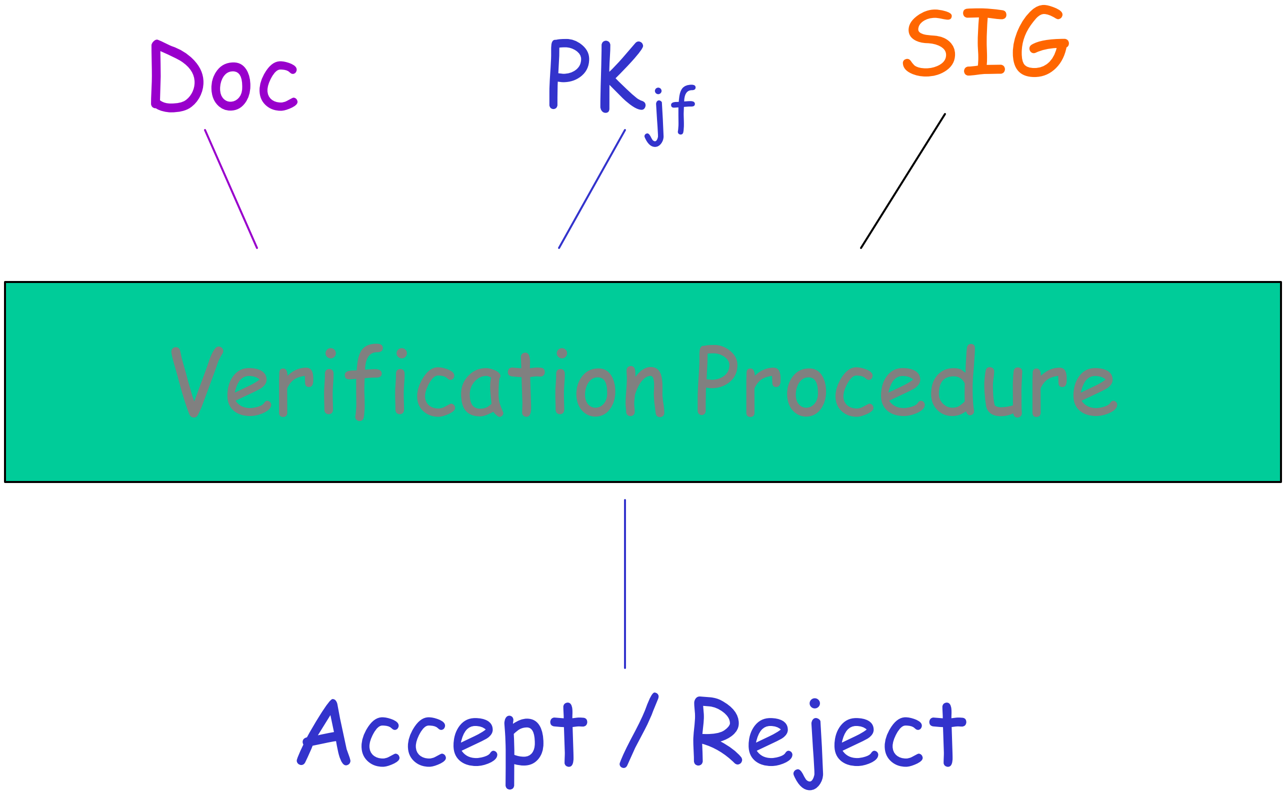


Doc

SK_{jf}

Signature Procedure

SIG



Doc

PK_{jf}

SIG

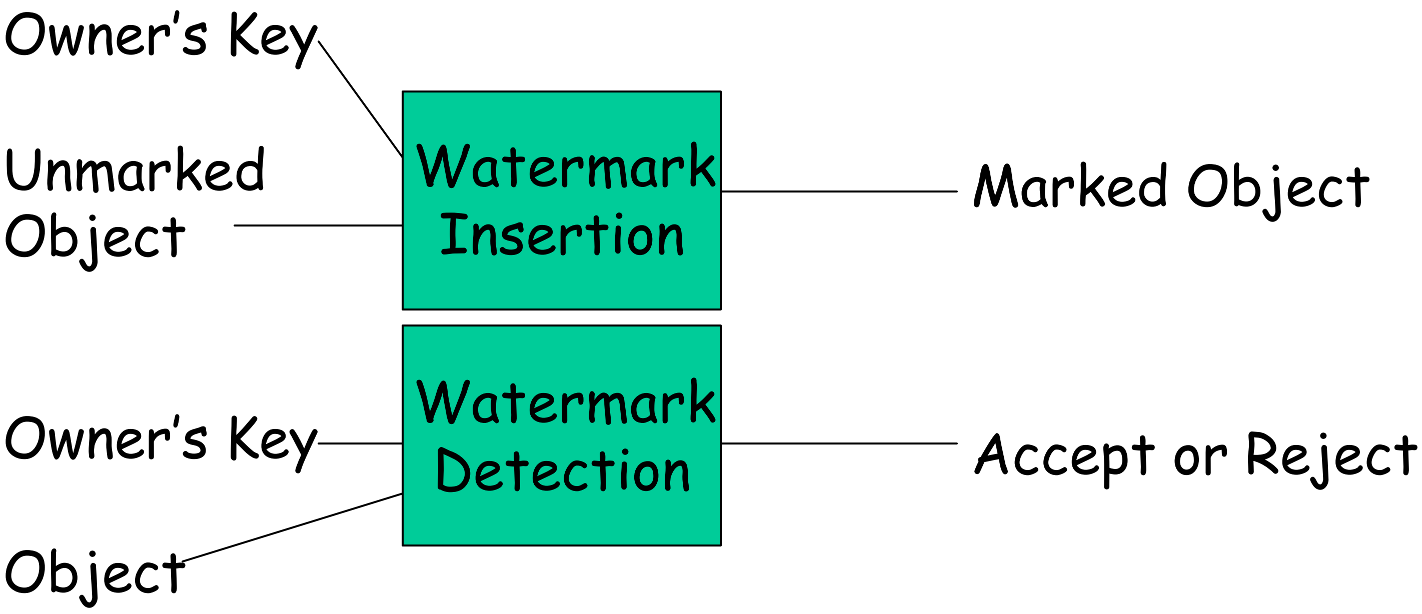
Verification Procedure

Accept / Reject

Examples

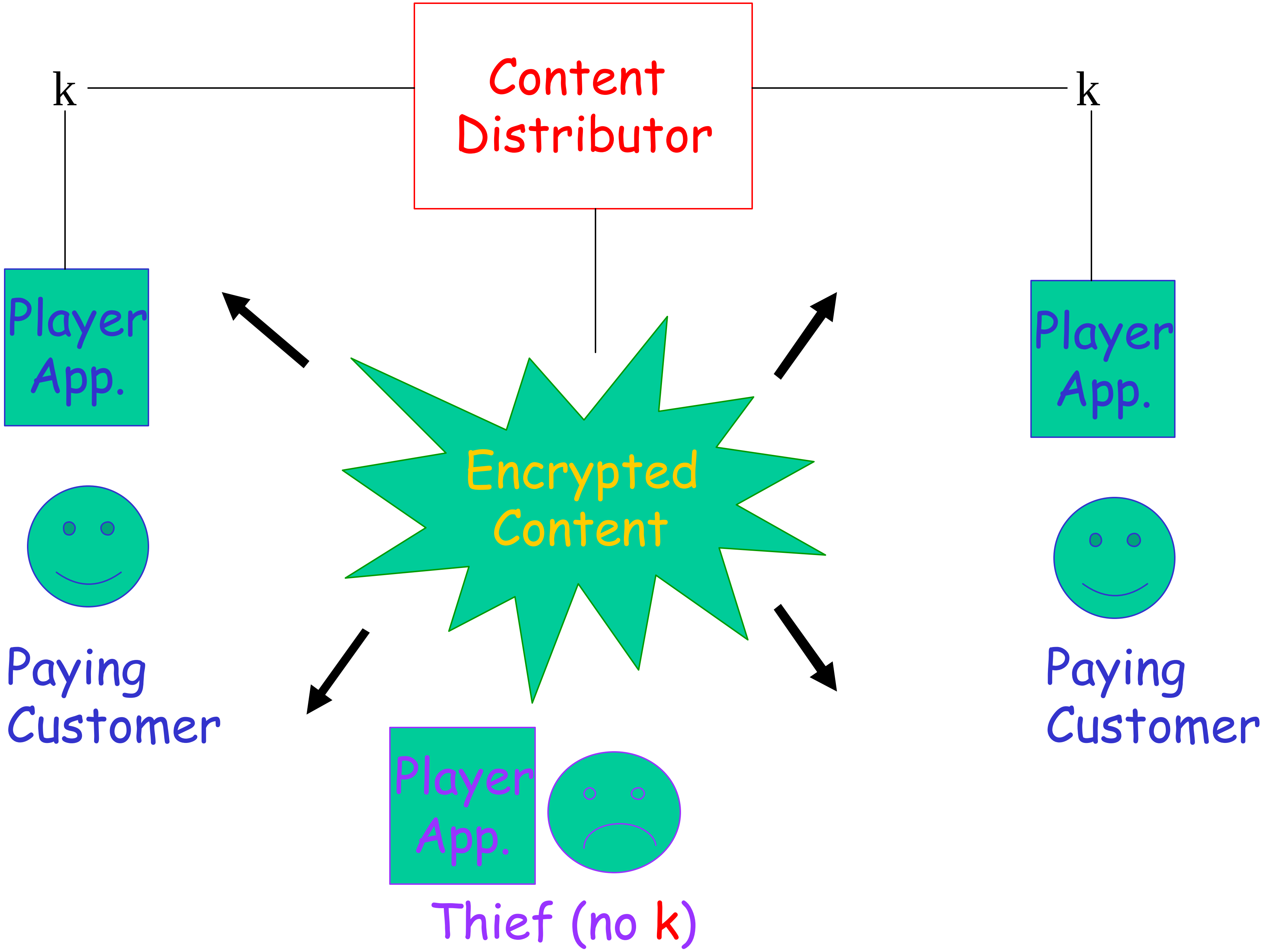
- RSA
- El Gamal
- DSA
- McEliece

Watermarking



Note similarity with and difference from digital signature scheme.

Open Problem: Public-key watermarking.



k

Content Distributor

k

Player App.

Player App.

Encrypted Content

Paying Customer

Paying Customer

Player App.

Thief (no k)

Common Elements of Many TPSs

- Mass-Market broadcast content
  - Anyone can get ciphertext, which is broadcast on low-cost channel (e.g., web page, broadcast TV).
  - Encrypted once.
- Decryption key k sent only to paying customers on lower-bandwidth, higher-cost channel.

Possible Realization for Web Pages

- Customer U and content-server use basic security protocol, e.g., SSL, to create "session key" K_U and transfer payment from U to server.
- Server sends k' = E(k, K_U) to U.
- U's browser computes k = D (k', K_U), downloads encrypted content, decrypts it using k, and displays it.

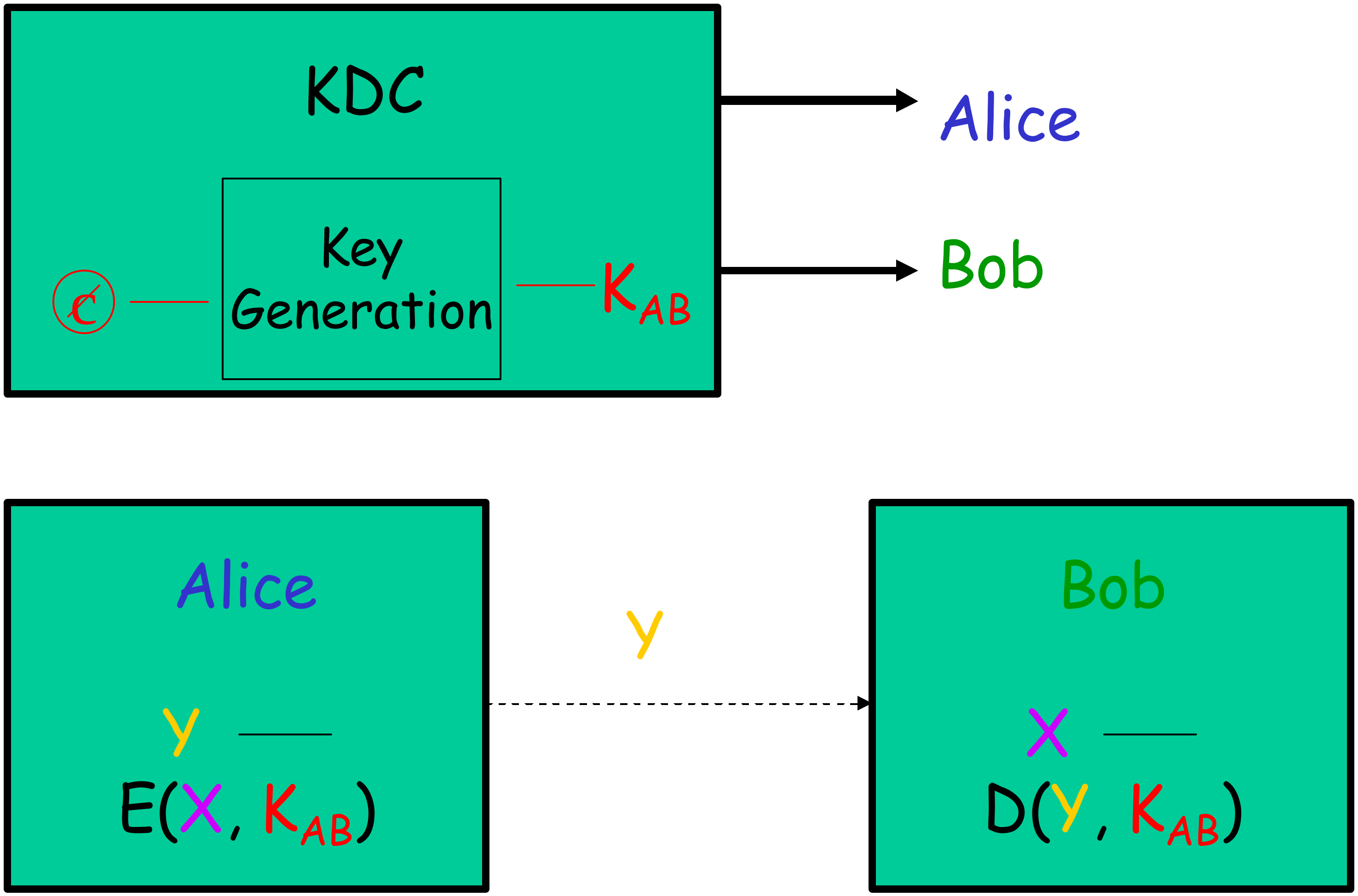
Possible Shortcomings

- Why can't U print, save, or otherwise redirect displayed content?

- Why can't a hacker steal k while it's in use?

- Interaction of browser with other local-network software, e.g., back-up system?

Crypto. Theory Myth:
Private Environments



KDC

¢

Key Generation

K_{AB}

Alice

Bob

Alice

y

$E(X, K_{AB})$

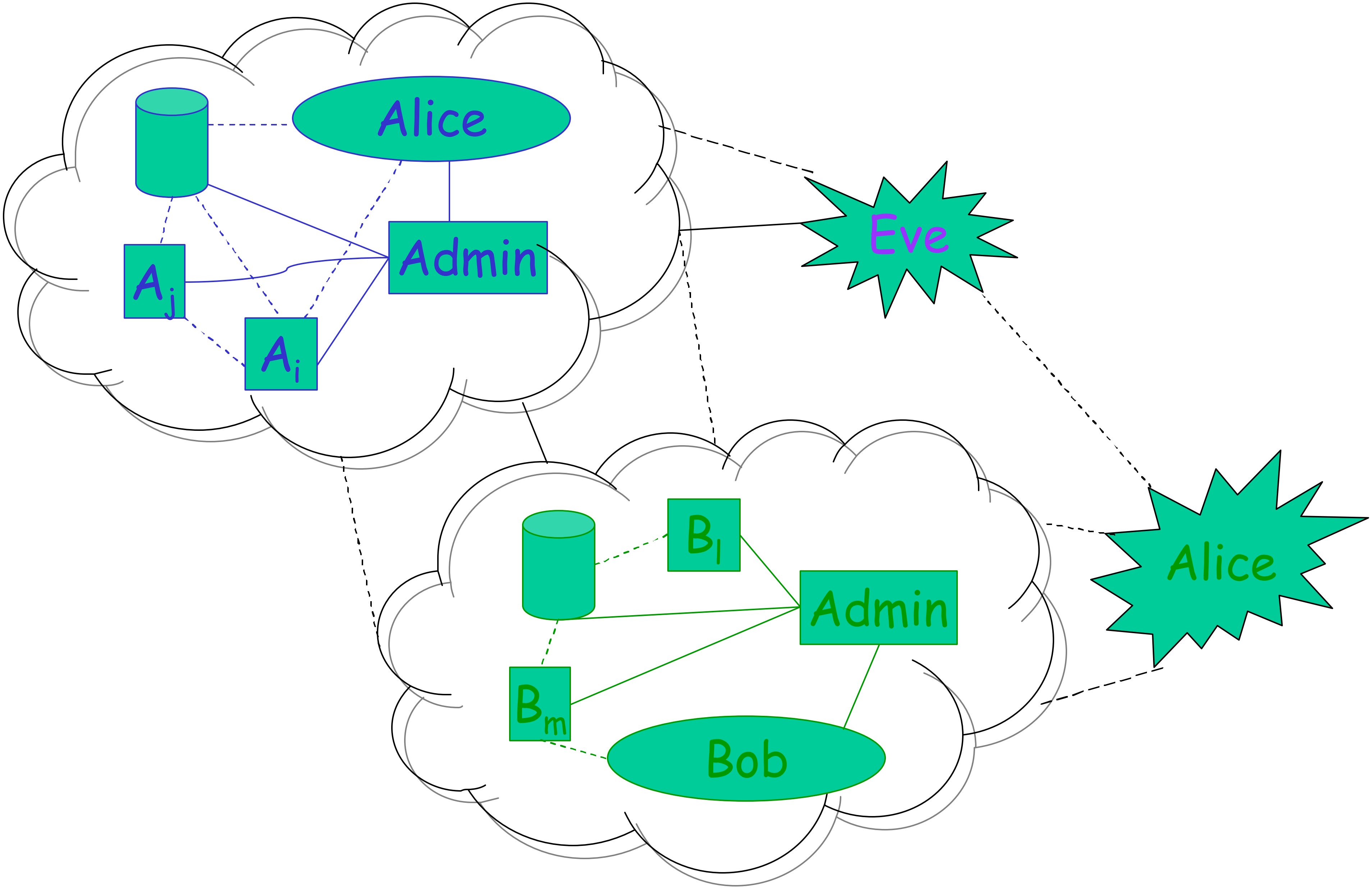
y

Bob

X

$D(y, K_{AB})$

Modern Computing Reality



Real Sources of Compromise

- Unwatched Terminals
- Administrative Staff Changes
- Misconfigurations
- OS Bugs
- Bad Random-Number Generators

Not sophisticated break-ins!

Possible Realization for Pay-TV

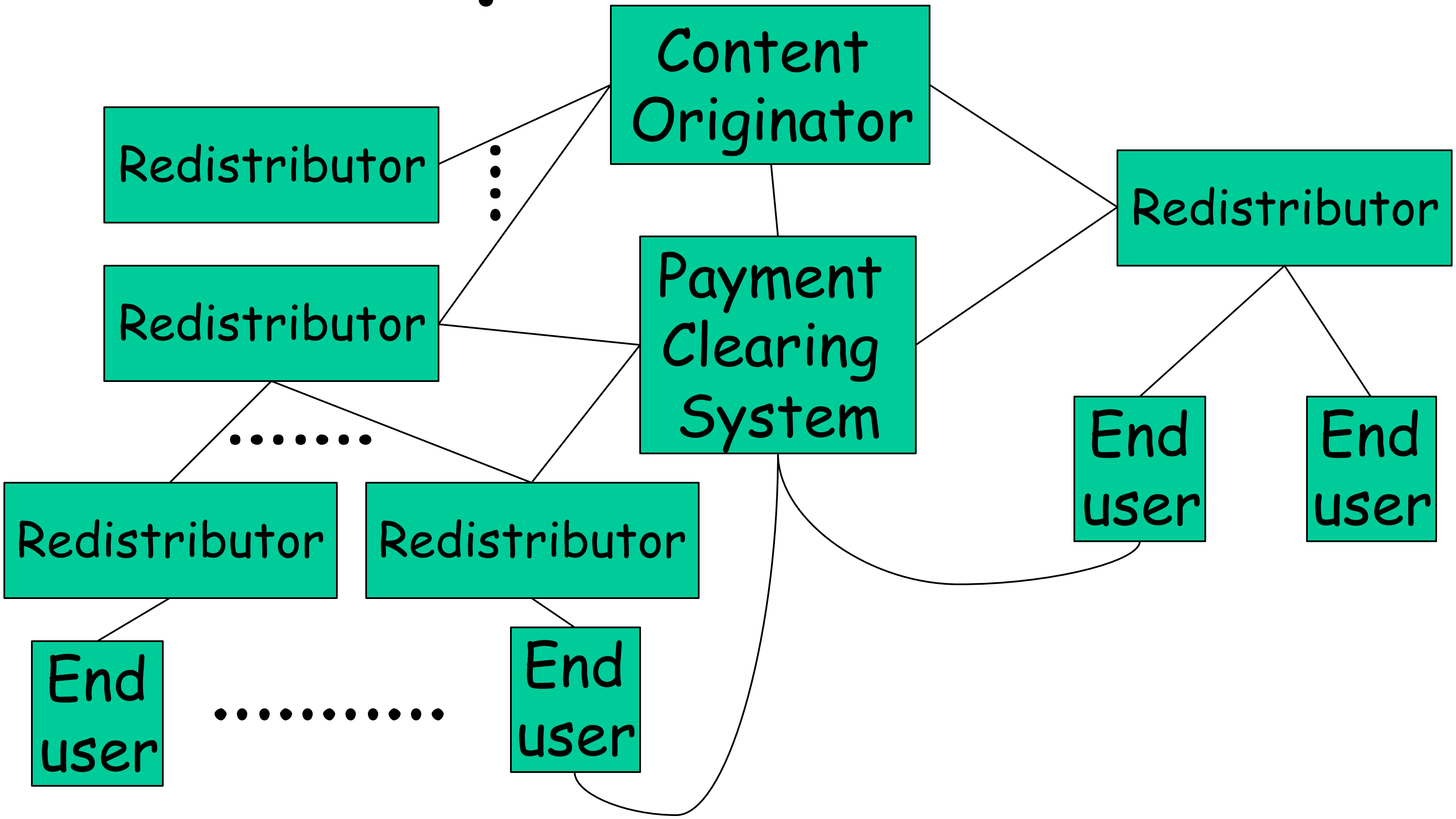
- K_{ui} is entered in ith "set-top box" when box is installed.
- $E(k, K_{u1}), \ldots, E(k, K_{uN})$ are broadcast with encrypted program.

Shortcoming: One broken box can be used to steal all future programs.

Uses of Watermarking in TPSs

- Broadcast of marked object, controlled distribution of keys. (Same architecture as in broadcast of encrypted content . . . and same shortcomings.)
- Web crawlers can search for unauthorized copies of marked objects.
- Unauthorized modification of marked objects can be detected by “fragile watermarking schemes.”
- Special-purpose devices can refuse to copy marked objects.

Superdistribution



- Content is packaged with “terms and conditions” that are checked by a “rights-management system” and can be augmented by value-adding middlemen.

Reading Assignment for September 27, 2001

- Appendix G of The Digital Dilemma (http://books.nap.edu/html/digital_dilemma/)
- The OpenLaw DVD/DeCSS Forum FAQ List (http://eon.law.harvard.edu/openlaw/DVD/dvd-discuss-faq.html)
- US v. Sklyarov FAQ from the Electronic Frontier Foundation (EFF) (http://www.eff.org/IP/DMCA/US_v_Sklyarov/us_v_sklyarov_faq.html)