CS155b: E-Commerce

Lecture 2: Jan. 11, 2001

Course Overview

Telephone Network

- Connection-based
- Admission control
- Intelligence is “in the network”
- Traffic carried by relatively few, “well-known”, communications companies

Internet

- Packet-based
- Best effort
- Intelligence is “at the endpoints”
- Traffic carried by many routers, operated by a changing set of “unknown” parties

Business Question: How to price Internet Service?

Technical and Business Question(s): How to provide different QoS levels and how to charge for them?

Technical, Business, and "Policy" Question: Does "intelligence at the endpoints" make sense for a mass-market public infrastructure?

Shift to Internet Causes

- Changes in existing businesses
  (e.g., telepresense)
- New ways to do old kinds of business
  (e.g., WWW-based retail)
- New kinds of businesses
  (e.g., Internet "infrastructure" providers)

As an infrastructure for communication, business, and almost all forms of human interaction, the Internet is new, rapidly changing, and inherently less manageable and controllable that older infrastructures.

Leads to problems with:

- Privacy
- Authenticity
- Accountability

Security Technologies

- Encryption
  - Symmetric Key
  - Public Key
- Signature
- PKI
- Rights Management
- Time stamping
- Secure Containers

References

- D. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Ration, 1995
- G. Simmons (ed.), Contemporary Cryptology: The Science of Information Integrity, IEEE Press, NY, 1992.
- A, Menezes et al., Handbook of Applied Cryptography, CRC Press, Boca Ration, 1997.
- IACR Publications:

  J. Cryptology, Crypto Proceedings,

  Eurocrypt Proceedings

  http://www.iacr. org

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
  - Government (especially export)
  - 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}

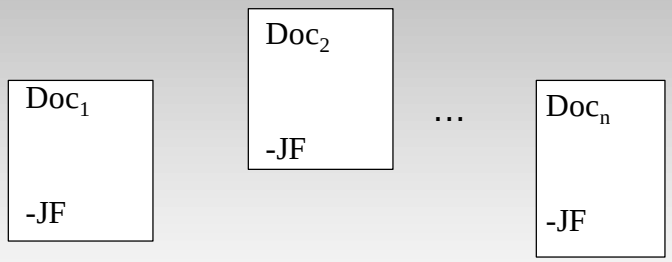
y <-- $E(x, PK_{bob})$

Alice -->Bob: y

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

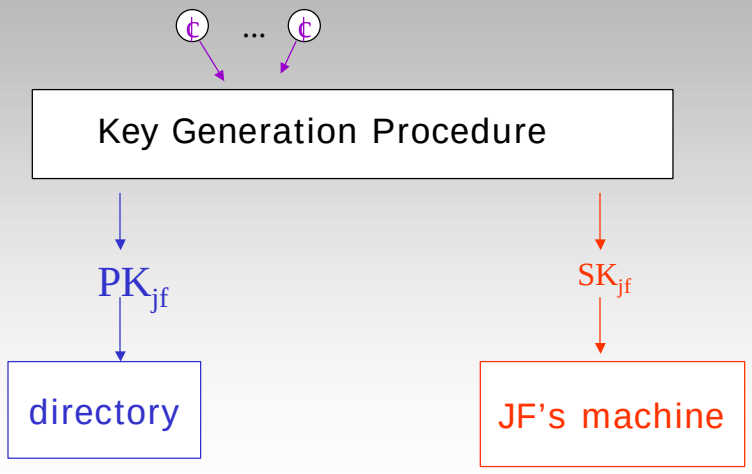
(Eve does not know SK_{bob})

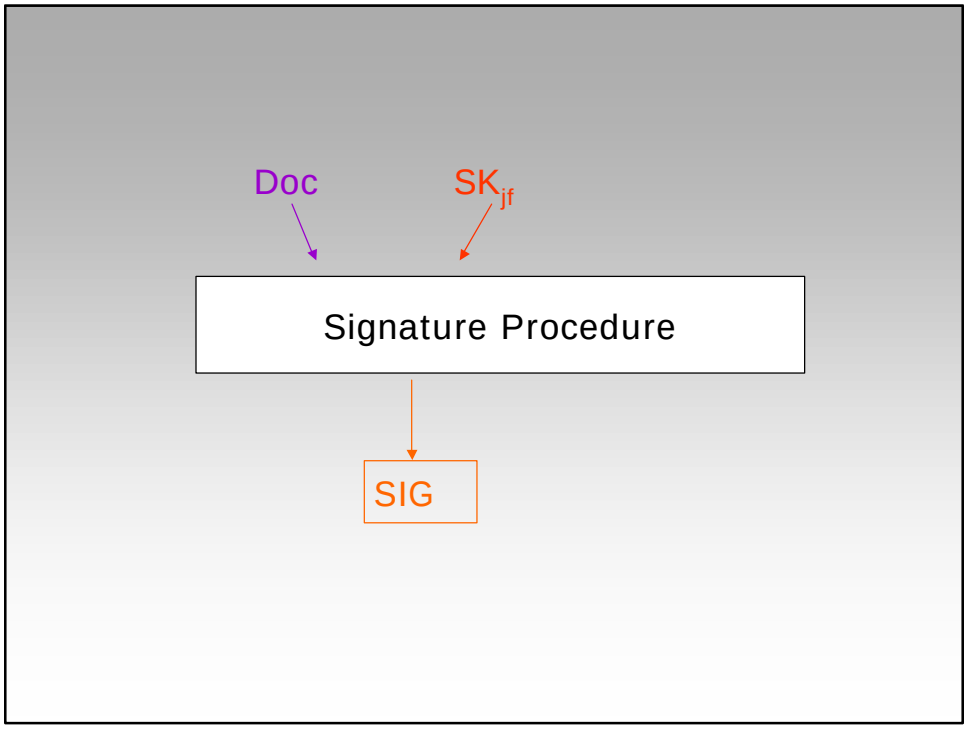
Digital Signatures

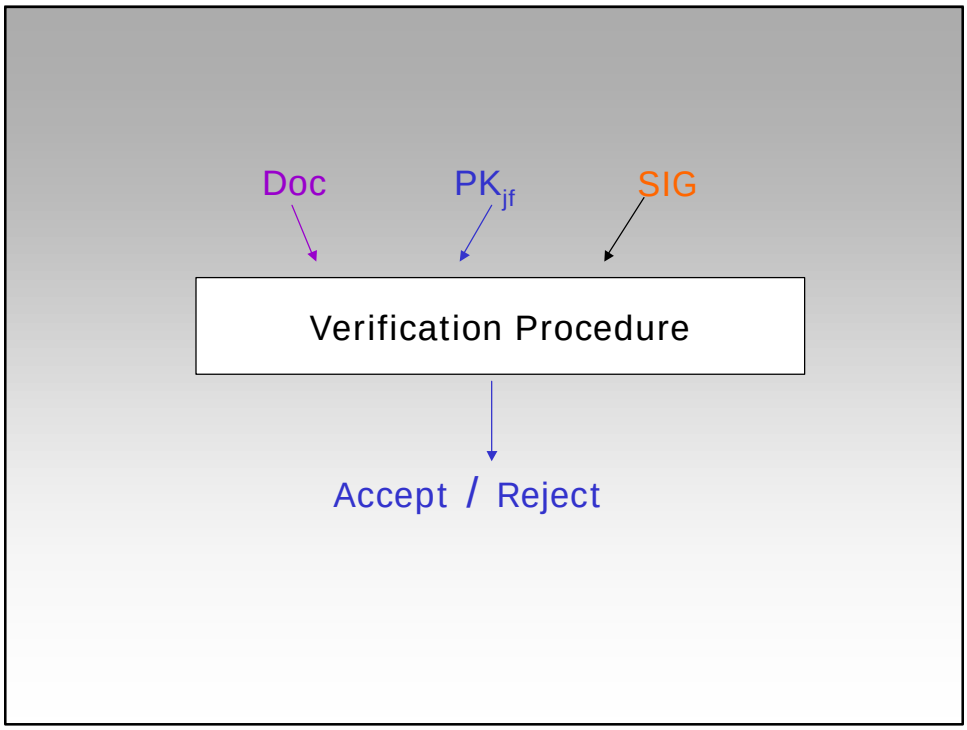


Trickier than the paper “analogue”

3-part Scheme



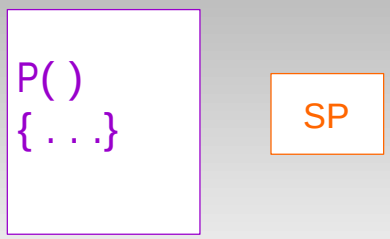

Doc
SK jf
Signature Procedure
SIG


Doc
PK jf
SIG
Verification Procedure
Accept / Reject

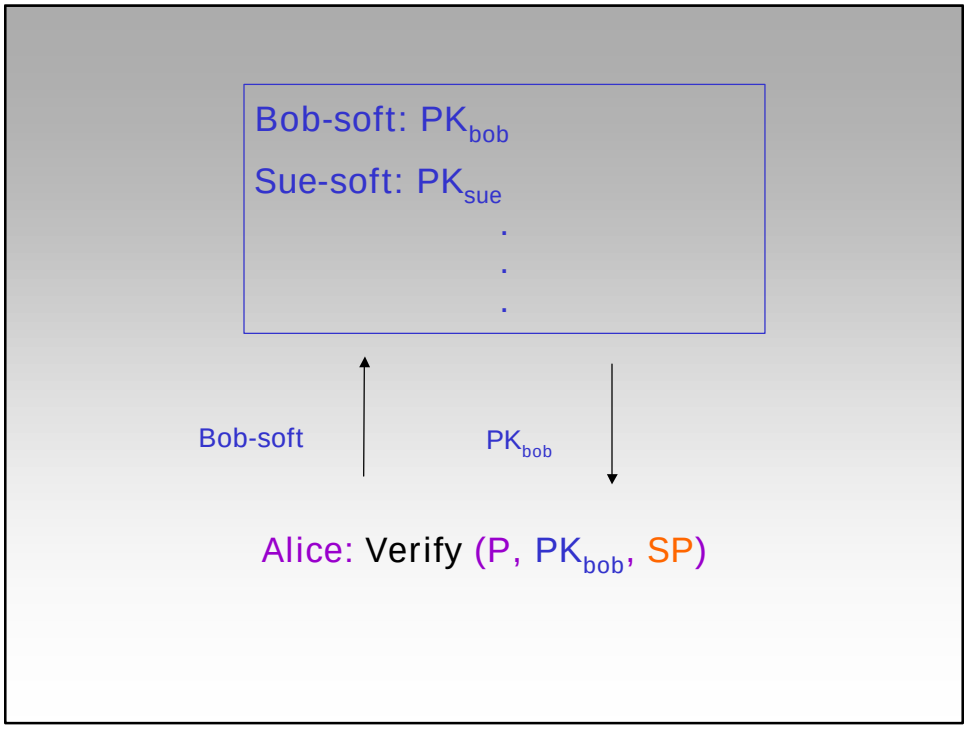
Examples

- RSA
- El Gamal
- DSA
- McEliece

http://www.bob-soft.com



$SP = signature(P, SK_{bob})$



New Potential Problem

- Is PK_{bob} the “Right Key”?
- What does “Right” mean?

Traditional Meaning

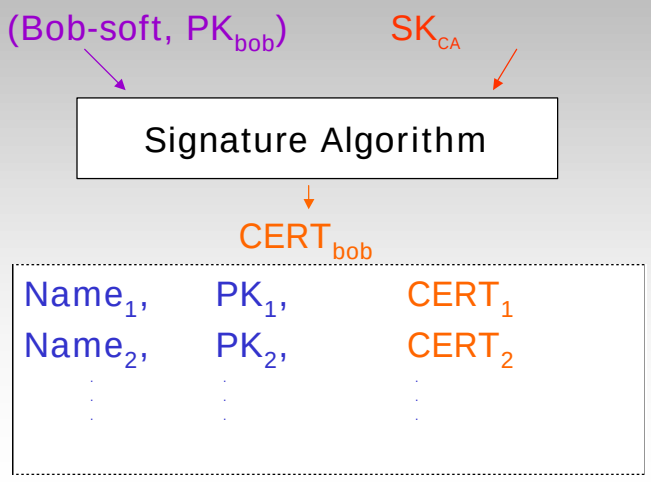
Bob-soft ↔ PK_{bob}

Accurate?

Traditional Solution

Alice's Computer PK_{CA}

Bootstrapping Trust



- Technical Question: Is this the right PK?
- Business Question: Can you make money selling public-key certificates?
- Political Question: Crypto export
- Legal Question: Do we have a right to use encryption? To some form of “electronic privacy”?

Changes in the Technology and the Economics of Publishing

- Computers and Digital Documents
- WWW-based Publication
- Internet Distribution

Technical Question: Is copying, modification, and redistribution of copyrighted material now uncontrollable?

Business Question: Is it possible to make money distributing copyrighted material (e.g., popular music) over the Internet?

Technical and Business Questions

- To what extent do encryption, digital signature, and other well understood security technologies make Internet content distribution manageable and profitable?
  - What other technology is needed?
  - What is the role of “circumvention” in effective development and deployment of relevant technology?

Technical, Business, and Legal Questions

- Is current copyright law technically feasible to implement and deploy on the Internet? ("copy-centric," "fair use is a defense, not a right")
- To what extent is copyright compliance monitorable? To what extent should it be monitored?

Global Network vs. Local Expectations

- Intellectual Property Law
- Censorship
- Banking Law

WWW Searching

- Technical Question: How to do it?
  (short answer: Linear Algebra)
- Business Question: How to make a business out of it? What is the role of advertising?
- Legal and Ethical Question: What conclusions should be drawn about people (by, e.g., gov't, employers, insurance companies...) based on what they search for and what they find?

WWW-Based, B2C Retail

Business Question: What to sell?

Business Question: How to capture and use customer information?

- Massive scale
- Variable Quality
- Numerous Formats and Intermediaries

Business, Legal, and Ethical Question: Who owns transaction data? To whom can it legally be sold? What can legally done with it?

Technical and Business Question:Is there an inherent tradeoff between personalization/efficiency and privacy? (the “cookie” question)

WWW-Based, C2C Retail

Economics and CS challenge:

Auction Design

Technical Challenge: C2C payment systems, e.g., “Electronic Cash”?

WWW-Based, B2B "exchanges"

Economics and CS Challenge:

Market Design

Technical, Business, and Legal Question: Do "industry-sponsored" electronic market places promote monopoly and monopsony?

Reading Assignment for Jan. 16, 2001

- Appendix C of The Digital Dilemma
  (http://books.nas.edu/html/digital_dilemma/)
- "Rethinking the Design of the Internet: The end-to-end arguments vs. the brave new world" (Clark & Blumenthal)
  (http://itel.mit.edu:/itel/docs/jun00/TPRC-Clark-Blumenthal.pdf)
- Optional: Some of the other articles on http://www.sobco.com/e.132/reading/arch.html