

Outline

- Introduction
- Automatic cryptography
 - Link encryption
 - Secret key management
 - Virtual private networks with IPSEC
 - Public key management
- User controlled cryptography
 - World Wide Web security
 - Electronic mail security
 - Public key certificates

Copyright 1998 Richard E. Smith. All rights reserved.

August 13, 1998

ic3.fm - 1

User Controlled Cryptography

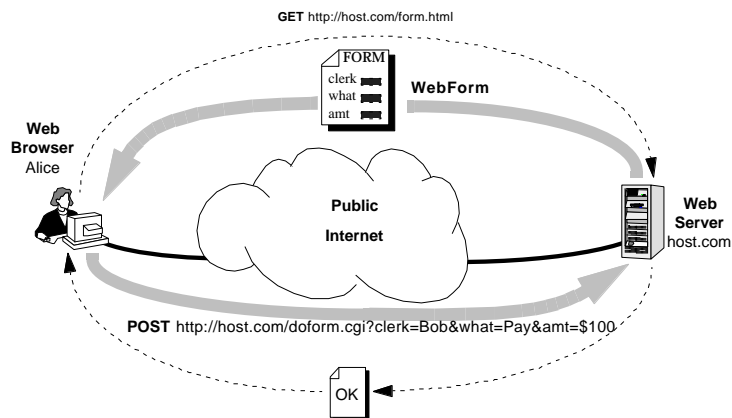
- General Features
 - Built into the application software
 - “Mixed” access to either general public destinations or to cryptographically protected destinations.
 - Little or no preplanning needed
- World Wide Web security with Secure Sockets Layer (SSL)
 - Mostly automatic protection with optional provisions of user overrides
- E-Mail Security
 - Several competing standards: PGP, S/MIME, PEM
 - Protection relies on user choice

August 13, 1998

ic3.fm - 2

World Wide Web Transactions

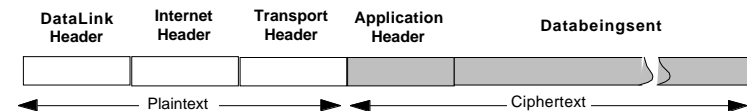
- Connections chosen and initiated by the Web Browser



August 13, 1998

ic3.fm - 3

Protecting Web Traffic

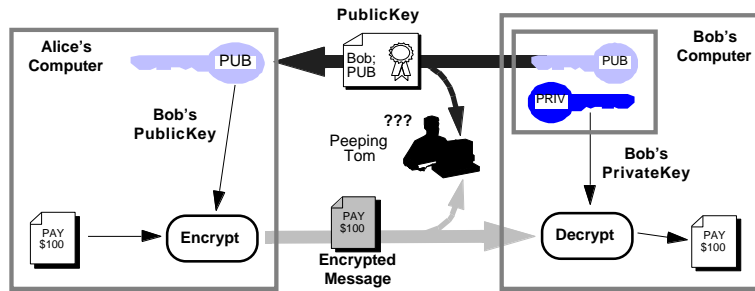


- Secure Sockets Layer (SSL) typically uses RSA for protection
- Protection is chosen by the “Web link” format.
 - Links with SSL protection contain “https:”
 - Web server can refuse a page unless it is retrieved using SSL
 - Some servers allow users to choose
- Protection is only applied to pages that really need protection
 - Example: credit card transactions versus advertisements

August 13, 1998

ic3.fm - 4

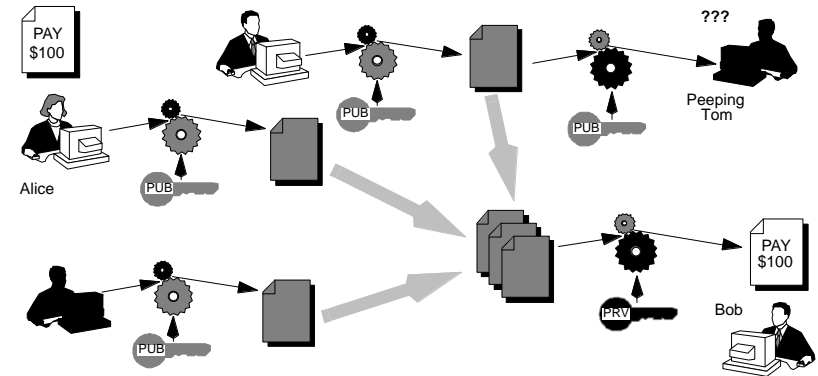
RSA for Encryption



August 13, 1998

ic3.fm - 5

Using RSA for Encryption

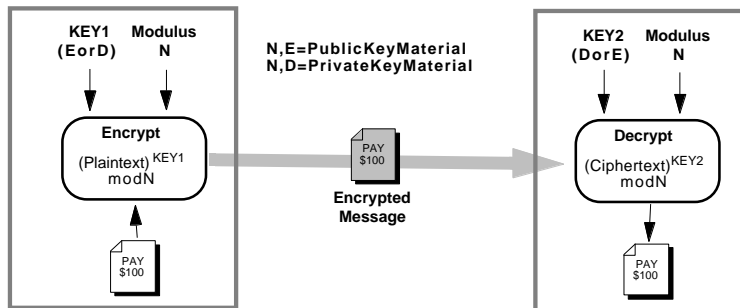


- Anyone with Bob's Public Key can encrypt messages to him
- Only Bob's Private Key can decrypt the messages

August 13, 1998

ic3.fm - 6

How RSA Works



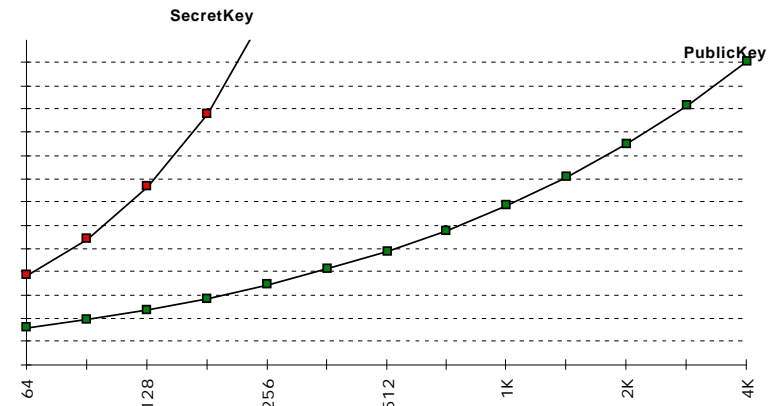
- Public key encryption uses "E" for KEY1 and "D" for KEY2
- Digital signatures use "D" for KEY1 and "E" for KEY2

August 13, 1998

ic3.fm - 7

Relative Strength of Keys

- Longer public keys can resist attack as well as secret keys



August 13, 1998

ic3.fm - 8

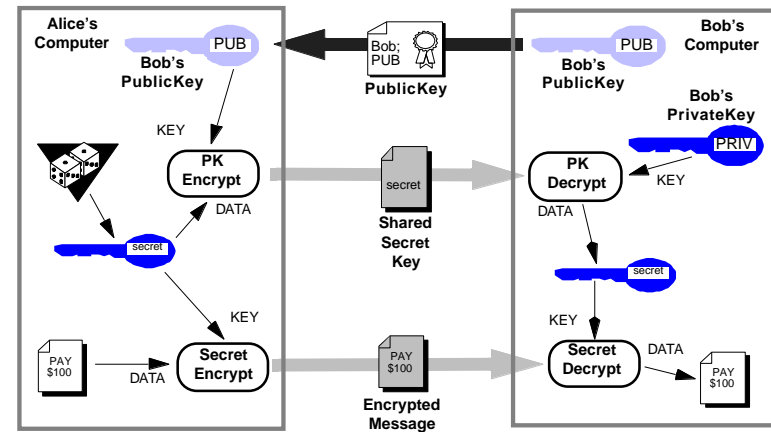
Weaknesses in Public Key Math

- Idiosyncratic usages produce mathematical weaknesses, giving attackers an **entering wedge**
 - Short plaintext can be cracked by taking the cube root of N in typical applications (public key = 3)
 - Private key can be cracked if its public key is relatively large
 - Dictionary attack if many similar messages are encrypted
 - Combine a “chosen ciphertext” encrypted message with an unknown encrypted message to crack the unknown one
 - Keys based on pseudo-primes will crack easily
- The solution: standard computation and formatting techniques that factor out the vulnerabilities: the Public Key Cryptography Standards (PKCS)

August 13, 1998

ic3.fm - 9

Key Distribution with RSA



August 13, 1998

ic3.fm - 10

Public Key versus Secret Key

- The following table reviews the relative benefits of Secret Key and Public Key techniques for key management.

| | Secret Key | Public Key |
|----------------------------|-------------------|---------------------|
| Size of Network | Few Hosts | Many Hosts |
| Network Organization | Centralized | Distributed |
| Network Membership | Preplanned | Unpredictable |
| Centralized Key Protection | Necessary | Not Necessary |
| Key Revocation | Fast and Accurate | Slow and Unreliable |
| Maturity | Mature Technology | New Technology |

August 13, 1998

ic3.fm - 11

Web Server Operation



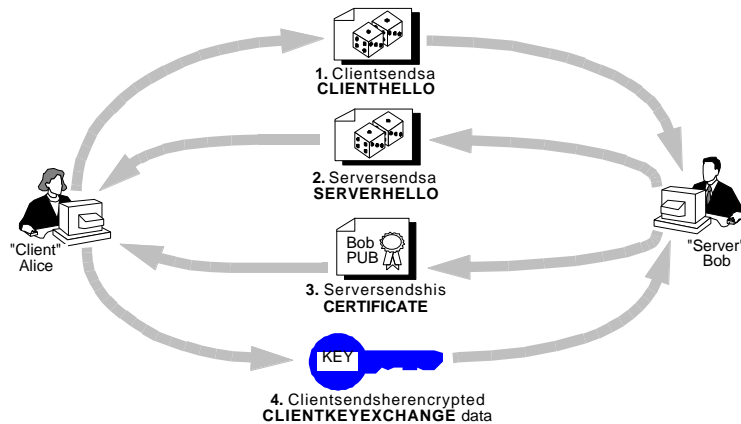
- User fills out a Web form. Pressing “SEND” will send the form to the server, protected by SSL
- The server reformats the form’s contents into a database transaction, and sends it to the order processing database.
- The database performs the transaction, and sends its reply.

August 13, 1998

ic3.fm - 12

SSL Key Exchange Protocol

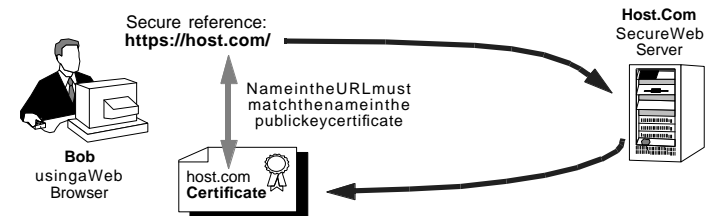
- Typically uses RSA encryption to protect the secrets



August 13, 1998

ic3.fm - 13

Authenticating the Server



- The server provides its "public key certificate" which contains its public key and its host name, and a digital signature
 - Host name in the Web link must match the certificate
- Client authentication uses any conventional method

August 13, 1998

ic3.fm - 14

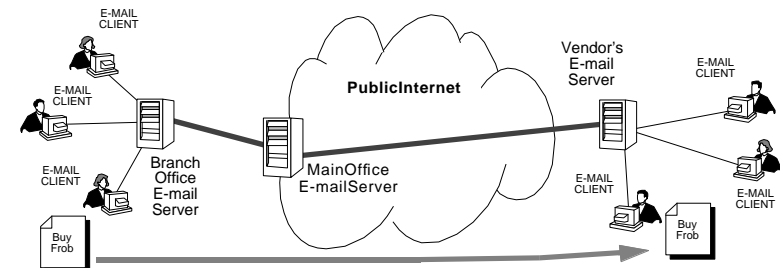
Web Server Security Recommendations

- Protocol Recommendations
 - SSL Version 3 is the best choice today: availability, level of security, widespread support.
 - Emphasize message integrity -- the biggest losses probably come from forged messages, not sniffed ones.
 - If you use passwords to authenticate clients, be sure to use encryption that can protect the passwords, or use a one time password product (Safeword, SecurID, etc.)
- Server Recommendations
 - Keep it simple -- complexity breeds errors.
 - The server system is also a target of attack, and is often easier to penetrate than even "exportable" encryption.

August 13, 1998

ic3.fm - 15

Internet Electronic Mail

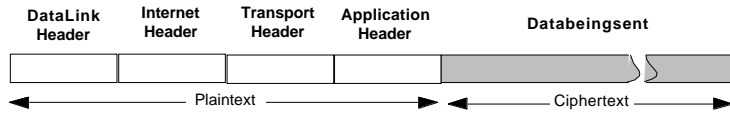


- Provides the most connections between users and sites
- E-mail may be "relayed" through different networks and "reformatted" to interact with proprietary e-mail products.

August 13, 1998

ic3.fm - 16

Protecting E-Mail

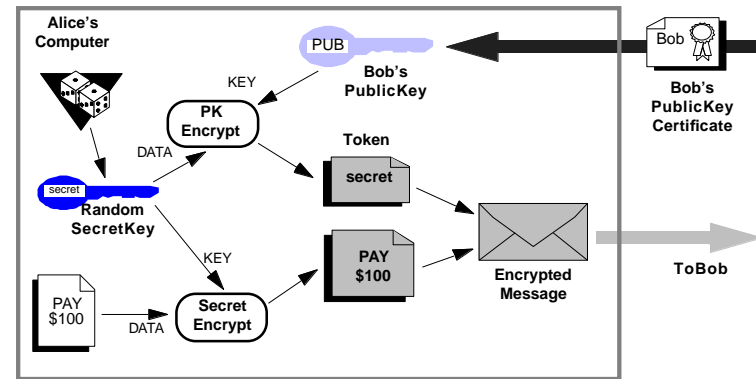


- Typically it only protects the contents of the e-mail message
 - This allows relaying through different e-mail systems.
 - Allows messages to be saved in a secure state
- User controlled protection
 - Benefits: interoperability with non-secure destinations, efficiency
 - Problem: accidentally omitting protection when it is needed.
- Digital signatures are used for off-line message authentication

August 13, 1998

ic3.fm - 17

Off-Line Message Keying

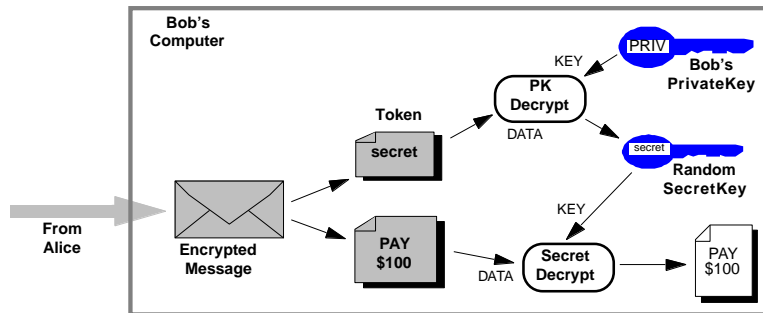


- With the certificate, a real time connection is not needed

August 13, 1998

ic3.fm - 18

Receiving E-mail

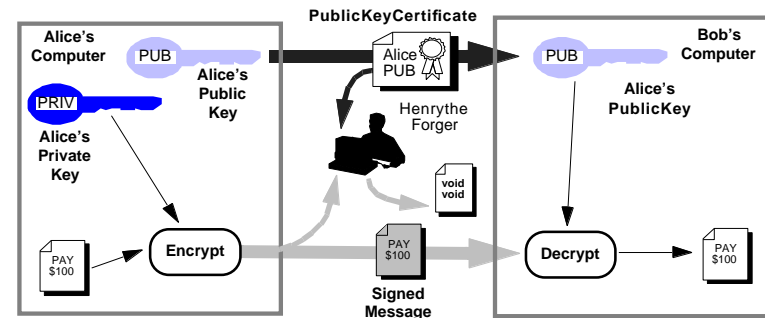


- Bob's private key decrypts the "token" encrypted with his public key.
- The "token" contains the secret key for that message.

August 13, 1998

ic3.fm - 19

Digital Signature

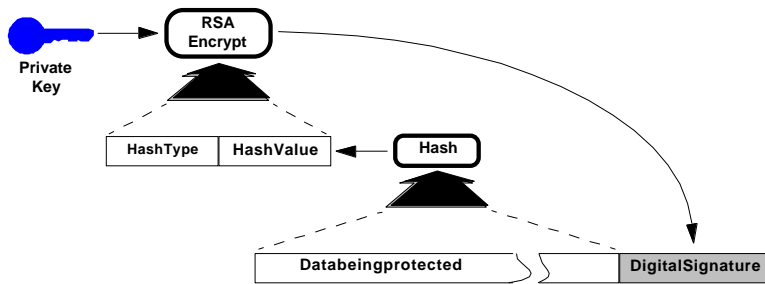


- Only Bob's Private Key can produce the digital signature.
- Any copy of Bob's Public Key can verify the digital signature.

August 13, 1998

ic3.fm - 20

RSA Digital Signature

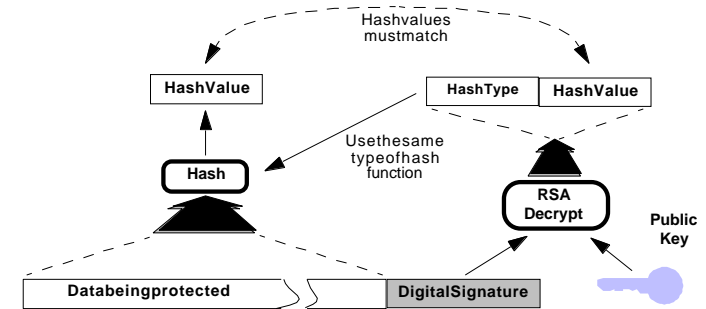


- Safest to hash the message before computing the digital signature value.
- Does not keep the message secret.

August 13, 1998

ic3.fm - 21

Validating the Digital Signature

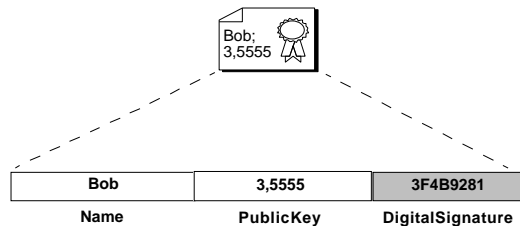


- Repeat the same hash computation
- Compare with the decrypted digital signature value

August 13, 1998

ic3.fm - 22

Public Key Certificates

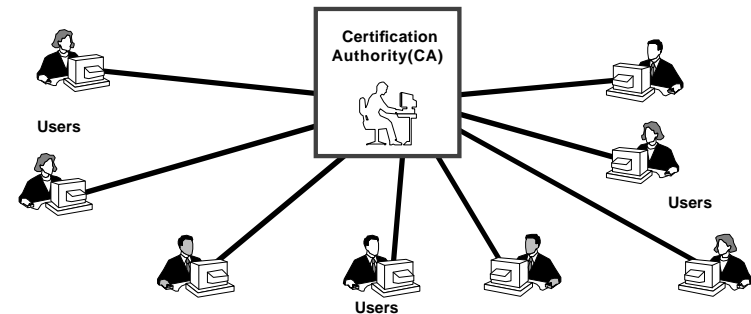


- Identifies the owner of a specific public key
 - Detect attempts to substitute one public key for another
- “Certificate Authority” applies the digital signature that validates the certificate.

August 13, 1998

ic3.fm - 23

Authentication of Certificates

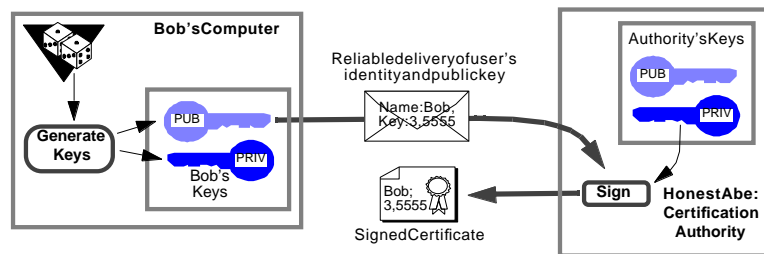


Use the authority's Public Key to validate all of the certificates used by a particular enterprise.

August 13, 1998

ic3.fm - 24

Generating a Certificate



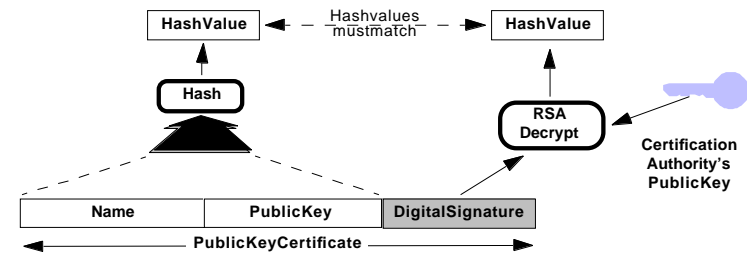
- The user generates a public and private key pair.
- The user keeps the private key secret, and sends a copy of the public key safely to the certificate authority.
- The certificate authority signs the certificate.

August 13, 1998

ic3.fm - 25

Checking a Certificate

F

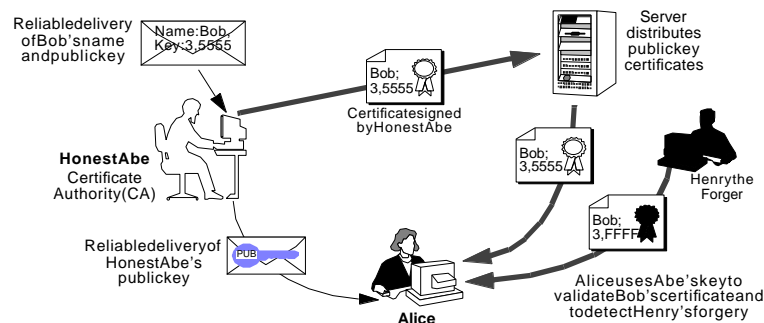


- Compute a hash over the public key and the owner's name.
- Decrypt the digital signature to retrieve the original hash.
- Both hashes will match if the certificate is authentic.

August 13, 1998

ic3.fm - 26

Overview of the Process



- Any trusted third party can be the "certificate authority" in theory. This yields the "web of trust" approach to certification.

August 13, 1998

ic3.fm - 27

Secure E-Mail Recommendations

- E-Mail Protocols
 - Use a recognized, "open" e-mail protocol.
 - Review any published information about problems with the protocol, and adapt your usage to maintain protection. \
 - Candidate protocols: PGP, S/MIME, PEM
- E-Mail Processes
 - Use digital signatures, since forgery is often the biggest risk.
 - Promote encryption as needed to keep essential secrets.
- Public Key Certificates
 - Select a certification discipline that fits your needs.
 - "Web of trust" is widely used today, but has limitations.
 - Commercial products for certificate authorities from Netscape

August 13, 1998

ic3.fm - 28