




Computers and Society

More Encryption

Chris Brooks

Department of Computer Science
University of San Francisco



Review

- Symmetric-key encryption
 - One key used to encrypt and decrypt
 - Encryption based on bit transposition and rotation.
 - Brute force search of keyspace needed to break
 - Challenge: how to distribute keys for new communications?

Review

- Asymmetric-key encryption
 - Separate keys used for encryption and decryption
 - Encryption based on modular arithmetic
 - Security is based on factoring large numbers.
 - Slower, larger keys needed.

Breaking RSA in practice

- RSA is the most well-known public-key algorithm.
- RSA systems has sponsored a series of challenges to crack RSA.
- RSA-512 broken in 1999.
- Estimate: capability grows by 13-14 bits (about 4 digits) a year.
- At this rate, 1024-bit RSA will be secure until about 2037.
- Question: How long does your data need to be secure?

Digital signing

- Alice wants to send Bob a message. She also wants Bob to be able to verify that it really came from her.
- She can encrypt the message with her private key and send it to Bob.
- Anyone can use her public key to read the message.
- Only Alice (or someone with her private key) can encrypt a message that can be read with her public key.
- This is called a *digital signature*; if Alice's private key is secure, then she must have sent the message.
- We can combine encryption and digital signing.

Validating with Hash Functions

- To sign a document, I compute its hash, encrypt that with my private key, and send the encrypted hash along with the original document as plaintext.
- The receiver hashes the plaintext and then uses my public key to verify that I was the one who sent the document.
- Can also detect tampering.

Combining Public and Secret Keys

- Since public-key encryption/decryption is slow, it's not very practical for large data transfers, such as SSL or HTTPS.
- Secret-key systems work better, but a method is needed to exchange keys.
- Public-key encryption is often used to synchronize secret session keys.

Combining Public and Secret Keys

- A generates a secret key and sends it to B, encrypted with B's public key.
- For handshaking, include a random number.
- B decrypts the message and has the secret key.
- For handshaking, B encrypts the random number with A's public key and returns it.

Key distribution

- Public-key encryption assumes that your public key is “well-known.”
- How does this happen in practice?
- A possible attack:
 - Alice goes to Bob’s website to get his public key.
 - An attacker sits in the middle, intercepts the request, and provides a fraudulent public key. The attacker can now impersonate Bob.

PKI

- For real-world applications, a complex web of software systems is required to ensure security.
- This is referred to as a Public Key Infrastructure (PKI).
- Focus shifts from provable protocol properties to system design.
- One of the primary functions of a PKI is the establishment of trust between users with no prior history.
- A *certificate authority* can provide this, serving as a trusted third party.

PKI

- A certificate authority has a number of functions within a PKI
 - Authentication
 - Key generation
 - Key revocation
- Many commercial entities serve as CAs
 - Verisign, Visa, GoDaddy

Certificate Authorities

- A Certificate Authority will wrap a user's public key in a certificate.
 - X.509 is most common standard.
- Contains the user's identity and public key.
- Signed with the CA's private key.
- Risk is shifted:
 - Previously: could unknown user A be compromised?
 - Now: could the CA be compromised?

PKI models

- Hierarchical
 - One root CA
 - Considered able to “vouch for” itself.
 - Scalable and fast
 - Requires setup in advance
- Distributed (Web of Trust)
 - No root CA
 - Users are able to authenticate each other
 - Same approach as P2P software
 - Highly redundant, but not very efficient.

SET

- SET (Secure Electronic Transaction) is a protocol developed by Visa and Mastercard.
- Uses a public-key system to ensure secure payment.
- Provides confidentiality, data integrity, authentication of cardholder and merchant.
- Establishes a hierarchical public-key infrastructure
- Public keys are used to exchange symmetric keys.

Dual Signatures

- SET prevents information leakage through the use of dual signatures.
- I want to buy a car and need the bank to transfer the funds.
- I don't want the dealer to see my bank balance
- I don't want the bank to see the terms of the deal.
- I only want the money to be transferred if my offer is accepted by the car dealer.

Dual Signatures

- I generate a message digest (hash) for each message and sign them.
- I then concatenate the digests and sign that.
- I send each party their message, plus the concatenated version.
- If the dealer accepts my offer, she sends the digest of the offer to the bank.
- Bank can concatenate this digest with the digest of the authorization I sent them to verify authenticity.
- Both parties can confirm that the other message is authentic, but can't know the contents.

Steganography

- One challenge with encryption is secrecy.
 - An attacker will typically know that you are sending an encrypted message.
- *Steganography* is the science of embedding a secret message within another message.
- Secret is carried innocuously within a harmless-looking wrapper.
- Useful when an encrypted message might draw suspicion.
- One use of steganography is the embedding of watermarks

Watermarks

- Traditionally, a watermark has been used to verify the authenticity of a document.
- Difficult to reproduce.
- Tampering will destroy watermark.
- Driver's Licenses, diplomas, official letterhead.
- More recently, used to track or prevent redistribution
 - TV logos

Digital Watermarks

- Three purposes:
 - Ensure authenticity of digital goods
 - Should be difficult to copy watermark.
 - Prevent unauthorized use/ensure copyright
 - Prevent copying
 - Should be difficult to remove watermark.

Watermarking Images

- Images (and sound and video) can be invisibly watermarked by altering the low-order bits.
 - For example, a 24-bit color image can represent 2^{24} different colors.
 - This is more than most monitors (or humans) can distinguish.
 - The low order bits are effectively noise.
- For example, by changing the lowest-order bit in each channel of each pixel in an image, we can embed 1 ASCII letter for every three pixels.

Authentication

- Proof of authenticity can be embedded into a digital good.
- Author generates a watermark, signs it, and embeds it.
- Commercial services might assign an ID
- Presence of watermark is advertised.
- User can verify, creator, date created, etc.
- Creators might also search the web for images bearing their watermark to track unauthorized usage.

Resistant Watermarks

- Just altering low-order bits is a fairly brittle approach.
 - To remove watermark, just open in Photoshop and resave.
- More sophisticated approaches involve manipulating elements of the image/sound/video itself.
 - Altering luminance, varying contrast
 - Embedding watermark in higher-order harmonics or in keyframes.

Legal Issues with Encryption

- Encryption and its use has been a controversial topic for many years.
- For many years (until late 90s), encryption algorithms were classified as munitions.
- This led to secure encryption algorithms being subject to export control.
- Companies had to develop two versions of their software, one for domestic use and one for export.
 - You might have seen T-shirts saying “This T-shirt is a munition”

```
print pack"C*",split/\D+/,`echo "16iII*o\U@{$/=$z;  
[(pop,pop,unpack"H*",<>)]}\EsMsKsN0[1N*11K  
[d2%Sa2/d0<X+d*1MLa^*1N%0]dsXx++1M1N/dsM0<J]dsJxp"|dc`
```

Legal Issues with Encryption

- An early case was the development of PGP in 1991.
 - Free public key encryption system.
 - Given away on the Internet. The US government felt that this was *de facto* export.
 - Zimmermann argued that this was a free speech/privacy issue.

Legal Issues with Encryption

- US companies found it difficult to compete with foreign companies.
- Electronic commerce was developing - encryption essential.
 - Less secure techniques had to be used.
 - Multiple versions of a product developed.
 - Most businesses just developed the weakest version of a product.
- 1995: Netscape's international encryption scheme (40 bit) broken.

Legal Issues with Encryption

- Controls weakened by late 90s.
 - Combination of business pressure and legal challenges.
 - Is encryption (or computer code) a form of speech?
 - Can academics write papers about research developments?
 - 1996: Computer code ruled to be speech.
 - 2000: US government drops most export restrictions.

Legal Issues with Encryption

- Why was US government so resistant?
 - Strong crypto already available abroad.
 - Extra work for NSA - more potential messages to be decoded.
 - Prevent the adoption of standards
 - Also eases NSA's job
 - Export rules required companies to disclose techniques to NSA, making them easier to crack.

Clipper Chip

- 1993: US government announces development of Clipper Chip.
- Uses a system known as key escrow.
- A copy of your private keys are kept with a third party.
- These keys could be accessed with a court order.
- Intended government standard for computer and telephone communications.

Clipper Chip

- Actual algorithm kept secret.
 - No one could use it without providing keys to escrow agents.
- Dropped due to technical flaws and political opposition.
- Replaced with key recovery schemes
 - Also useful if keys are lost.
- Mostly voluntary.

Issues

- Secrecy
 - As a government tool
 - Evaluating algorithms
- Public vetting has proved quite helpful at testing security schemes.
- Potential “back doors”
- Violation of constitutional rights.

Trust in Government

- The essential tension is between providing government with the tools to protect us and keeping them from the tools to oppress us.
- One's view of government affects where you stand in this debate.

Examples

- PGP is used by white supremacists to coordinate illegal activity.
- Journalists documenting human-rights abuses use PGP to encrypt their stories.
- Drug dealers use PGP to encrypt details of payment transfer.
- Political activists use PGP to coordinate demonstrations