

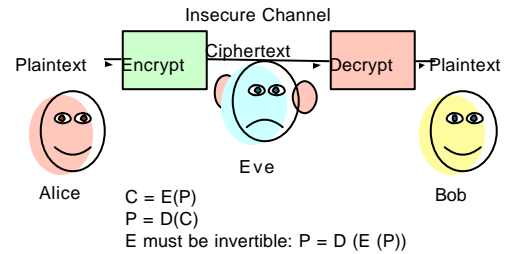
Encryption: How it works, why it (sometimes) doesn't, and what it can do

With a magnetic card and his dog Buddy's name as a password, President Clinton e-signed a bill Friday that will make electronic signatures as real as those on paper.

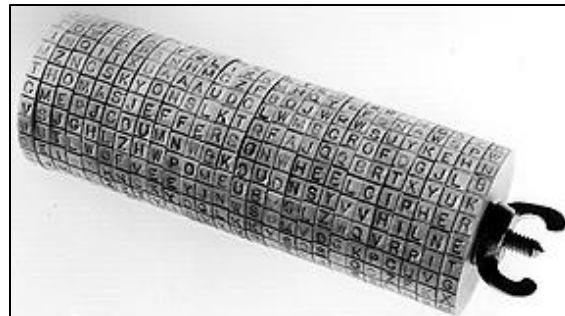
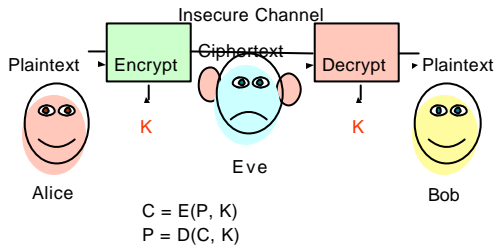
FoxNews, 30 June 2000

David Evans
evans@cs.virginia.edu

Terminology



"The enemy knows the system being used."
Claude Shannon



Jefferson Wheel Cipher



Enigma

- About 50,000 used by Nazi's in WWII
- Modified throughout WWII, believed to be perfectly secure
- Broken by Bletchley Park led by Alan Turing (and 30,000 others)
- First computer (Colossus) developed to break Nazi codes (but kept secret through 1970s)
- Allies used decrypted Enigma messages to plan D-Day

Modern Symmetric Ciphers

A billion billion is a large number, but it's not that large a number.
— Whitfield Diffie

- Same idea but:
 - Use digital logic instead of mechanical rotors
 - Larger keys
 - Encrypt blocks of letters at a time

DES [1976]

56-bit key
 $2^{56} = 72$ quadrillion

Can try 1 Trillion keys per second, break DES in < 1 day

19 Sept 2001 Cyberlaw: Encryption 7

Modern Ciphers

- AES (Rijndael) successor to DES selected last year
- 128-bit keys, encrypt 128-bit blocks
- Brute force attack
 - Try 1 Trillion keys per second
 - Would take 10790283070806000000 years to try all keys!
 - If that's not enough, can use 256-bit key
- No known techniques that do better than brute force search

19 Sept 2001 Cyberlaw: Encryption 8

Problem with all Symmetric Ciphers

How do Alice and Bob agree on K (without Eve hearing it)?

19 Sept 2001 Cyberlaw: Encryption 9

Padlocked Boxes

Alice

19 Sept 2001 Cyberlaw: Encryption 10

Padlocked Boxes

Alice's Padlock

Alice's Padlock Key

19 Sept 2001 Cyberlaw: Encryption 11

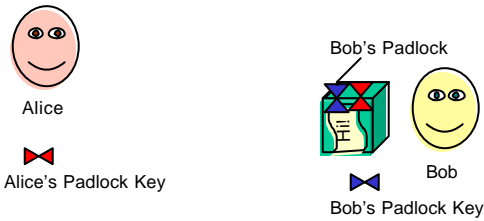
Padlocked Boxes

Alice's Padlock Key

Shady Sammy's Slimy Shipping Service

19 Sept 2001 Cyberlaw: Encryption 12

Padlocked Boxes

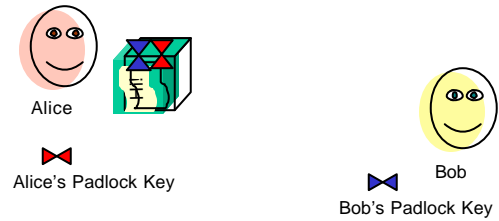


19 Sept 2001

Cyberlaw: Encryption

13

Padlocked Boxes

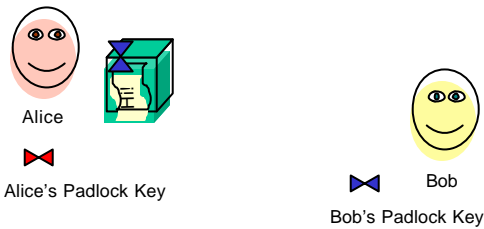


19 Sept 2001

Cyberlaw: Encryption

14

Padlocked Boxes

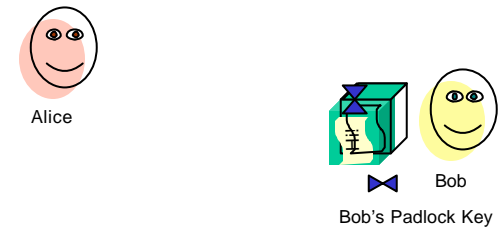


19 Sept 2001

Cyberlaw: Encryption

15

Padlocked Boxes

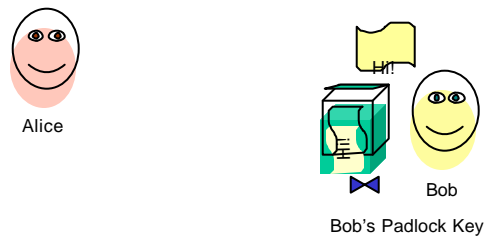


19 Sept 2001

Cyberlaw: Encryption

16

Padlocked Boxes



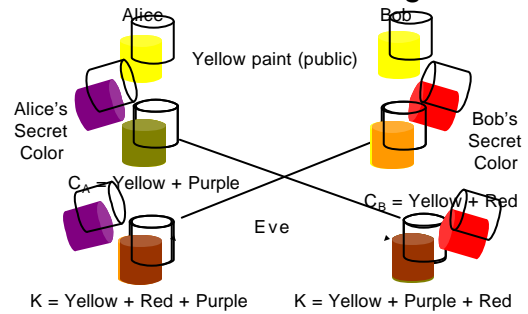
19 Sept 2001

Cyberlaw: Encryption

17

Secret Paint Mixing

Analogy due to Simon Singh, *The Code Book*.



19 Sept 2001

Cyberlaw: Encryption

18

One-Way Functions

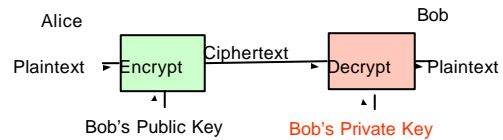
- Like mixing paint – easy to mix, hard to unmix
- Simple example:
 - Middle 100 digits of n^2 , n random 100 digit number
 - Given n , easy to calculate.
 - Given 100 digits, hard to find n .
- Trap-door one way function:
 - $D(E(M)) = M$
 - E and D are easy to compute.
 - Revealing E doesn't reveal an easy way to compute D

19 Sept 2001

Cyberlaw: Encryption

19

Public-Key Applications: Privacy



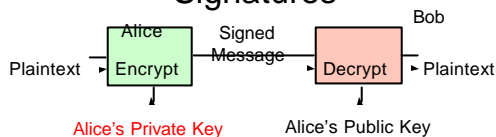
- Alice encrypts message to Bob using Bob's Private Key
- Only Bob knows Bob's Private Key \Rightarrow only Bob can decrypt message

19 Sept 2001

Cyberlaw: Encryption

20

Signatures



- Bob knows it was from Alice, since only Alice knows Alice's Private Key
- Non-repudiation: Alice can't deny signing message (except by claiming her key was stolen!)
- Integrity: Bob can't change message (doesn't know Alice's Private Key)

19 Sept 2001

Cyberlaw: Encryption

21

RSA

[Rivest, Shamir, Adelman 78]

$$E(M) = M^e \bmod n \quad \text{Public key } (e, n)$$

$$D(C) = C^d \bmod n \quad \text{Private key } d$$

e, d and n chosen so

$$M^{ed} \bmod n = M$$

$$D(E(M)) = E(D(M)) = M$$

19 Sept 2001

Cyberlaw: Encryption

22

Choosing e, d, n

Choose 2 secret primes p and q

$$n = p * q$$

$$e * d \equiv 1 \pmod{(p-1)(q-1)}$$

Depends on number theory theorems of Euler and Fermat

19 Sept 2001

Cyberlaw: Encryption

23

RSA in Perl

Until 1997 –
Illegal to show
this slide to
non-US
citizens!



19 Sept 2001

Cyberlaw: Encryption

24

Security of RSA

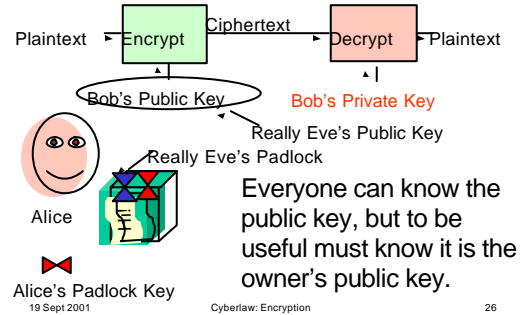
- n is public, but not p and q where $n = p * q$
 - If we can find p and q , easy to find d (private key)
 - Sounds easy: just need to factor n
 - 4th grade factoring: divide by 2, 3, 4, ...
- n is ~200 digits – would take quintillions of years
- Better algorithms known, but not much better

19 Sept 2001

Cyberlaw: Encryption

25

Key Management



19 Sept 2001

Cyberlaw: Encryption

26

Approach 1: Meet Secretly

- Alice and Bob meet secretly and swap public keys
 - If you can do that, might as well agree on a secret (symmetric key) instead
 - Doesn't work for Internet transactions

19 Sept 2001

Cyberlaw: Encryption

27

Approach 2: Public Announcement

- Publish public keys in a public forum
 - Append to email messages
 - Post on web site
 - New York Time classifieds
- Easy for rogue to pretend to be someone else
 - Forge email, alter web site, lie to New York Times

19 Sept 2001

Cyberlaw: Encryption

28

Approach 3: Public Directory

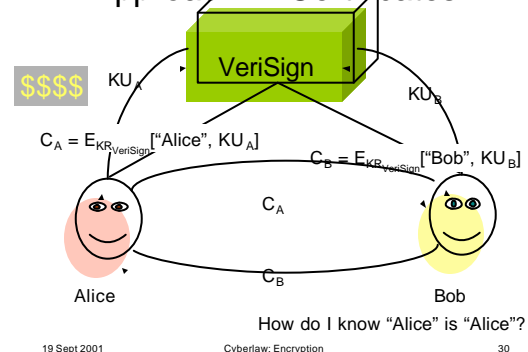
- Trusted authority maintains directory mapping names to public keys
- Entities register public keys with authority in some secure way
- Authority publishes directory
 - Print using watermarked paper, special fonts, etc.
 - Allow *secure* electronic access
 - Depends on secure distribution of directory's key

19 Sept 2001

Cyberlaw: Encryption

29

Approach 4: Certificates



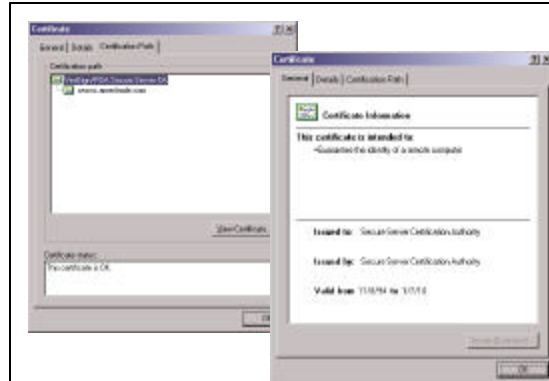
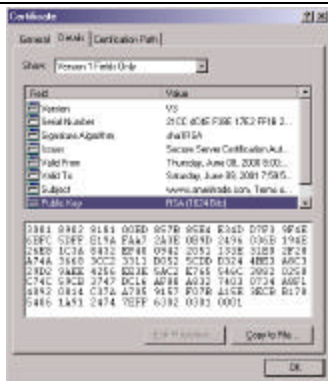
19 Sept 2001

Cyberlaw: Encryption

30



Data encrypted using secret key exchanged using some public key associated with some certificate.



Summary

- Cryptology can do a lot:
 - Keep secrets
 - Provide signatures
 - Anonymity, Money, Voting, Zero-Knowledge Proofs, etc.
- But, its not perfect:
 - Depends on humans not making mistakes
 - Tough to associate keys with principals

<http://www.cs.virginia.edu/evans/talks/cyberlaw.ppt>