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

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

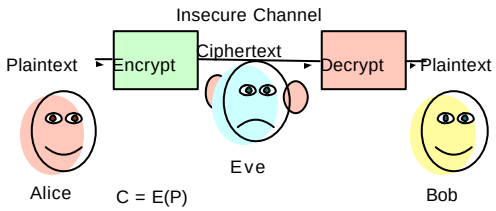
With a magnetic card and his dog Buddy's name as a password, President Clinton e-signed a bill Friday that will make electronic signatures as real as those on paper.

FoxNews, 30 June 2000

David Evans
evans@cs.virginia.edu
http://www.cs.virginia.edu/evans

University of Virginia
Department of Computer Science

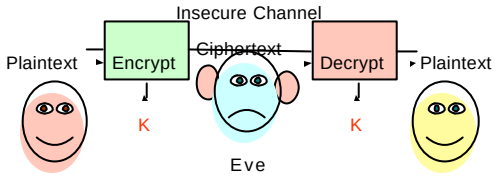
Terminology



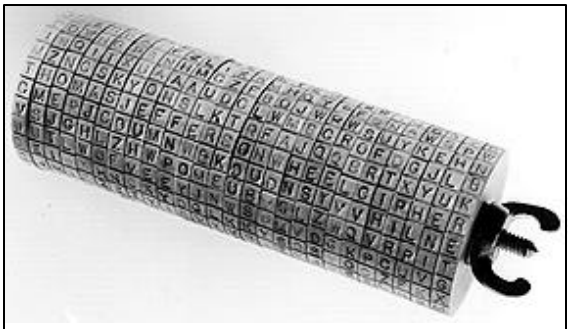
C = E(P)
P = D(C)
E must be invertible: P = D (E (P))

"The enemy knows the system being used."

Claude Shannon



C = E(P, K)
P = D(C, K)



Jefferson Wheel Cipher

Enigma

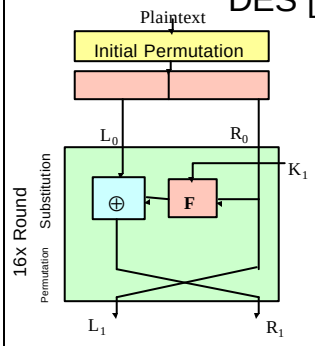
- About 50,000 used by Nazi's in WWII
- Modified throughout WWII, believed to be perfectly secure
- Broken by Bletchley Park led by Alan Turing (and 30,000 others)
- First computer (Collossus) developed to break Nazi codes (but kept secret through 1970s)
- Allies used decrypted Enigma messages to plan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



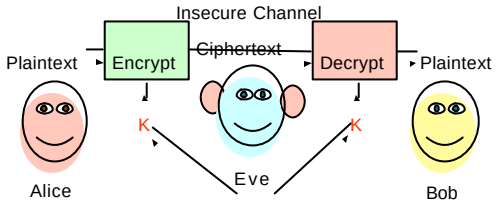
56-bit key
2^{56} = 72 quadrillion

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

Modern Ciphers

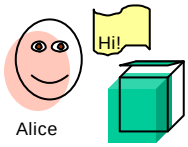
- AES (Rijndael) successor to DES selected last year
- 128-bit keys, encrypt 128-bit blocks
- Brute force attack
  - Try 1 Trillion keys per second
  - Would take 10790283070806000000 years to try all keys!
  - If that's not enough, can use 256-bit key
- No known techniques that do better than brute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

Problem with all Symmetric Ciphers

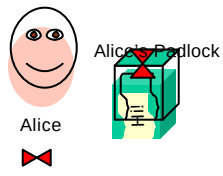


How do Alice and Bob agree on K (without Eve hearing it)?

Padlocked Boxes



Padlocked Boxes

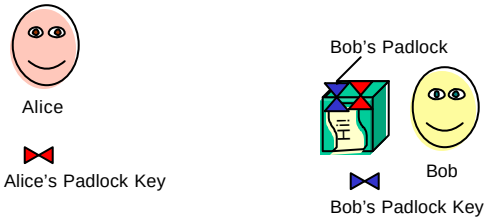


Alice's Padlock Key

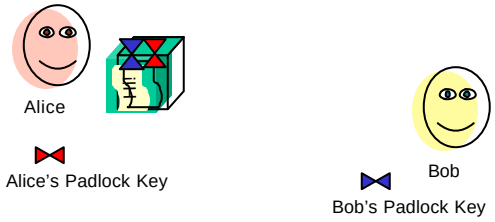
Padlocked Boxes

Alice's Padlock Key

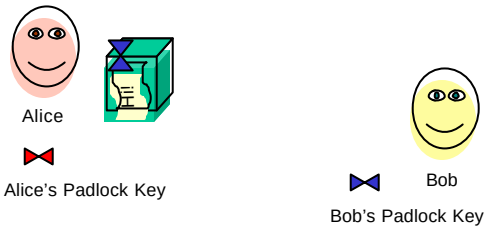
Padlocked Boxes



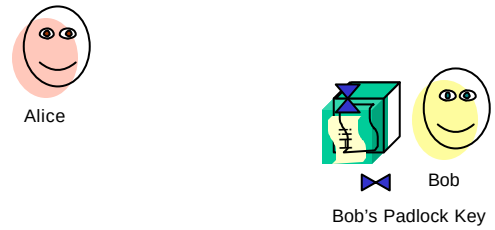
Padlocked Boxes



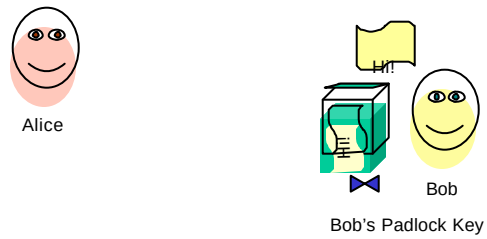
Padlocked Boxes



Padlocked Boxes

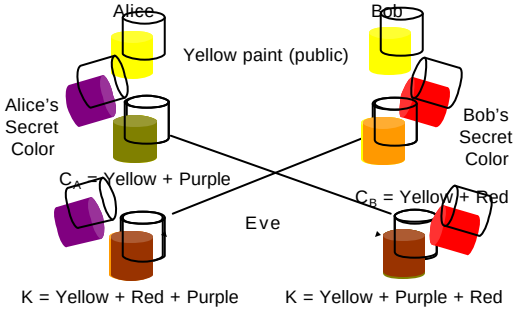


Padlocked Boxes



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

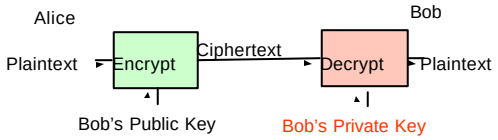
Secret Paint Mixing



One-Way Functions

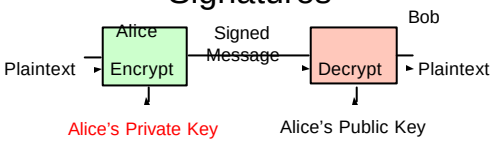
- Like mixing paint – easy to mix, hard to unmix
- Simple example:
  - Middle 100 digits of n^2, n random 100 digit number
  - Given n, easy to calculate.
  - Given 100 digits, hard to find n.
- Trap-door one way function:
  - $D(E(M)) = M$
  - E and D are easy to compute.
  - Revealing E doesn't reveal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

Public-Key Applications: Privacy



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

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)

RSA
[Rivest, Shamir, Adelman 78]

$E(M) = M^e \bmod n$ Public key (e, n)

$D(C) = C^d \bmod n$ Private key d

e, d and n chosen so

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

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

Choosing e, d, n

Choose 2 secret primes p and q

$$n = p * q$$

$$e * d \equiv 1 \bmod (p-1)(q-1)$$

Depends on number theory theorems of Euler and Fermat

RSA in Perl

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

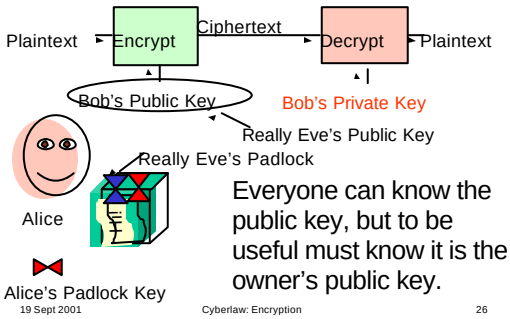
Security of RSA

- 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

Key Management



Everyone can know the public key, but to be useful must know it is the owner's public key.

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

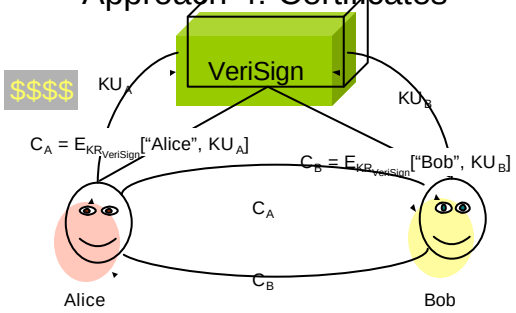
Approach 2: Public Announcement

- 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

Approach 3: Public Directory

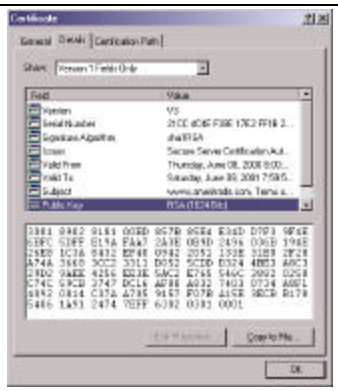
- Trusted authority maintains directory mapping names to public keys
- Entities register public keys with authority in some secure way
- Authority publishes directory
  - Print using watermarked paper, special fonts, etc.
  - Allow *secure* electronic access
    - Depends on secure distribution of directory's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

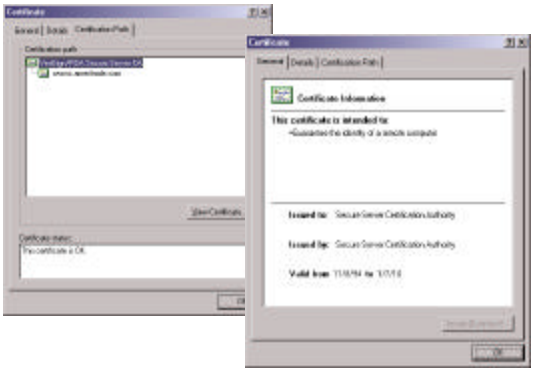
Approach ~~4: Certificates~~



How do I know "Alice" is "Alice"?

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