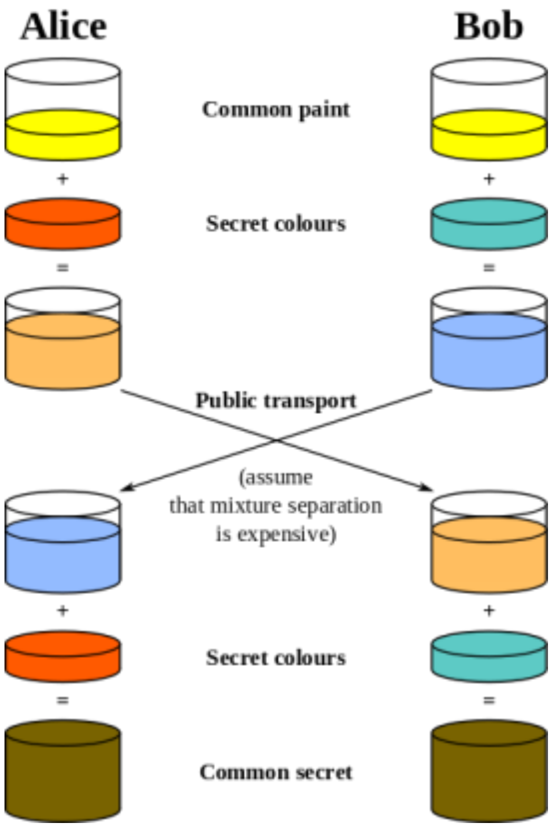
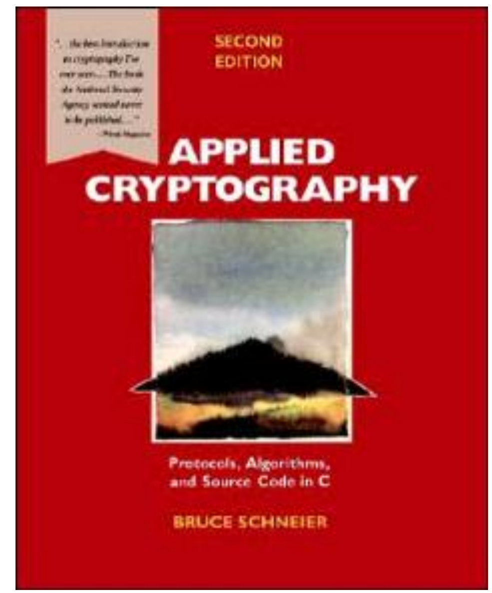
Modern Cryptography



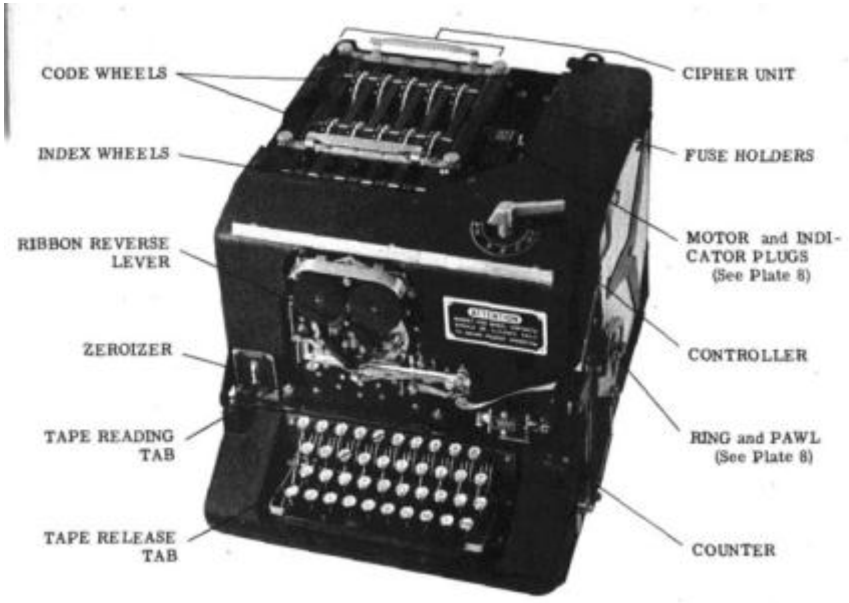


Overview

- Historical cryptography
  - WWII allied encryption
- Modern cryptography
  - Symmetric cryptography
    - DES/3DES
    - AES
  - Asymmetric cryptography
    - Diffie-Hellman key exchange
    - RSA

Allied encryption

- Typex
  - British Army and air force
  - 5 rotors
- ECM Mark II
  - Americans
  - 15 rotors



Navy Department, Office of Chief of Naval Operations, Washington, D.C.
CLASSIFICATION: CONFIDENTIAL Date: 27 Dec 1943
CARELESS COMMUNICATIONS COST LIVES
The following is a list of some of common violations of security principles:
DRAFTING:
Unnecessary word repetition
Unnecessary or improper punctuation
Plain language reply to encrypted dispatch
Classification too high
Precedence too high
Cancellation in plain language of an encrypted dispatch
ENCRYPTION:
"XYX" or "X"'s for nulls
"XX" & "KK" to separate padding from text
Same letters at both ends to separate padding from text
Continuity of padding
Seasonal and stereotyped padding
Repetition of generatrices (Ed. Note: CSP-845)
Systematic selection of generatrices (Ed. Note: CSP-845)
Using plain text column for encryption (Ed. Note: CSP-845)
Proper strips not eliminated as prescribed by internal indicator (Ed. Note: CSP- 845)
Improper set-up according to date
Using system not held by all addressees
Failing to use system of narrowest distribution
CALLS:
Enciphering indefinite call sign
Enciphering call signs of shore activities
CODRESS might have been used

Operation of the cipher machine is as important as the cipher itself!

Code talkers

- Machine based encryption
  - Heavy equipment
  - Slow to perform
- Code talking
  - Use Native American languages
  - Started in WWI with Choctaw
  - Improvise phrases for out-of-vocabulary words
    - "big gun" = artillery
    - "little gun shoot fast" = machine gun

Code talkers

- Navajo code talkers
  - WW II
  - Few outsides had learned the unwritten language
  - 3 line message, 20 seconds vs. machine 30 minutes
  - Compiled lexicon of 274 words + phonetic alphabet

http://library.thinkquest.org/28005/flashed/timemachine/courseofhistory/navajo-dic.shtml

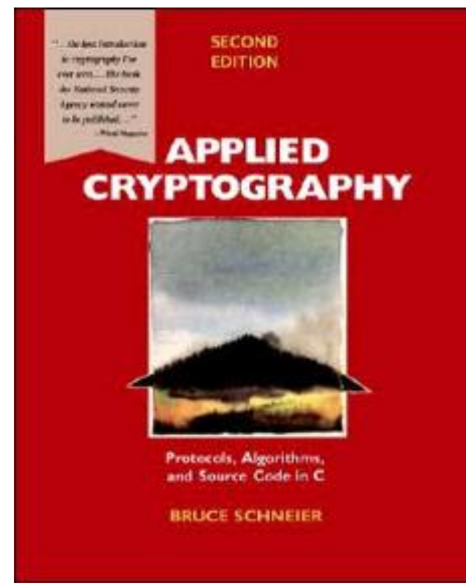
Modern cryptography

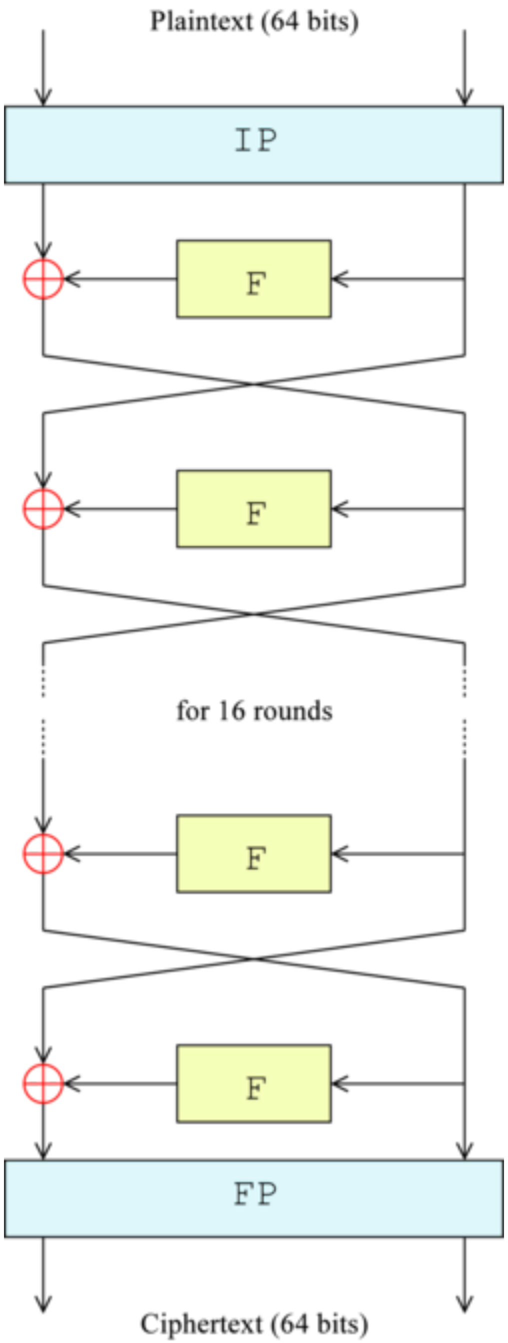
- Moving into computer age
  - Not limited to physical engineering constraints
    - Hundreds of rotors instead of 3
    - Changing in complex ways
  - Much faster
  - Scrambling at the bit level
- Symmetric encryption
  - What we've seen thus far
  - Encrypting message M with key K: $E_k(M) = C$
  - Decrypting ciphertext C with key K: $D_K(C) = M$
  - $D_K(E_K(M))=M$
  - Stream cipher (bit level) vs. Block cipher (multiple bytes)

DES

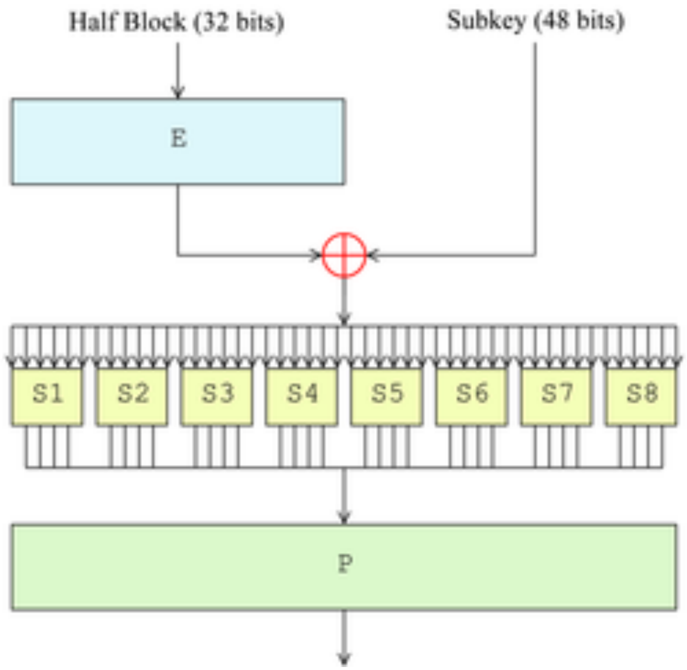
- Data Encryption Standard (DES)
  - NIST wanted a government-wide standard
  - Developed from IBM's Lucifer cipher
    - With "cooperation" from NSA
    - Improved S-boxes
    - Reduced key length from 64 to 48 bits
  - 1976 approved as a standard

> "DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure"
> -Bruce Schneier

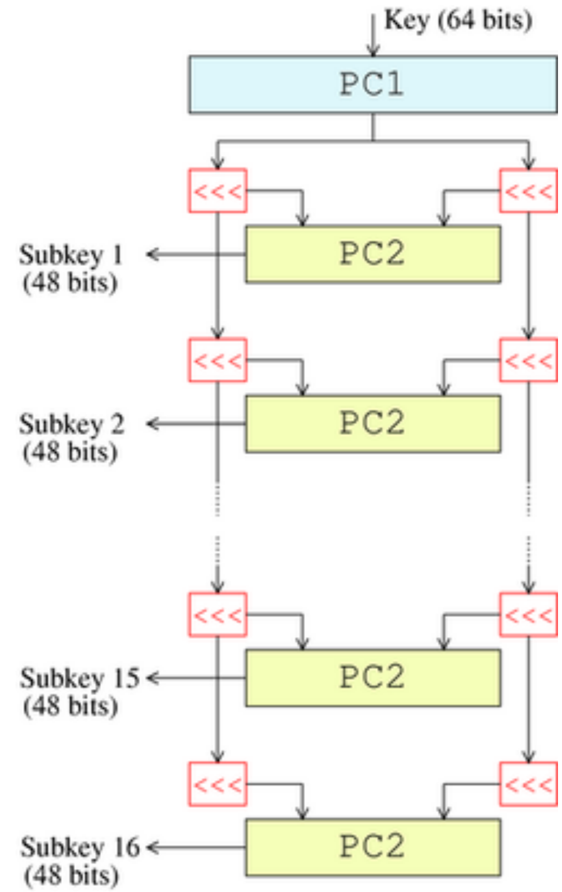




Plaintext (64 bits)
IP
F
F
for 16 rounds
F
F
FP
Ciphertext (64 bits)

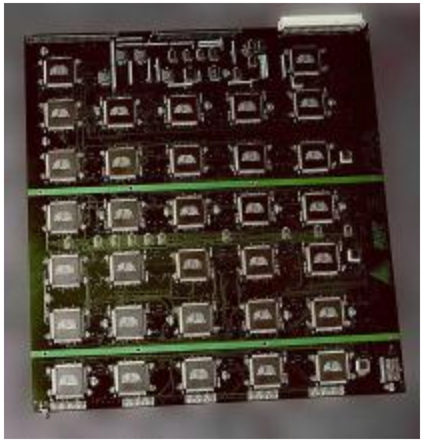


Half Block (32 bits)
Subkey (48 bits)
E
S1
S2
S3
S4
S5
S6
S7
S8
P



Key (64 bits)
PC1
<<<
<<<
PC2
Subkey 1 (48 bits)
PC2
Subkey 2 (48 bits)
PC2
Subkey 15 (48 bits)
PC2
Subkey 16 (48 bits)

Breaking DES



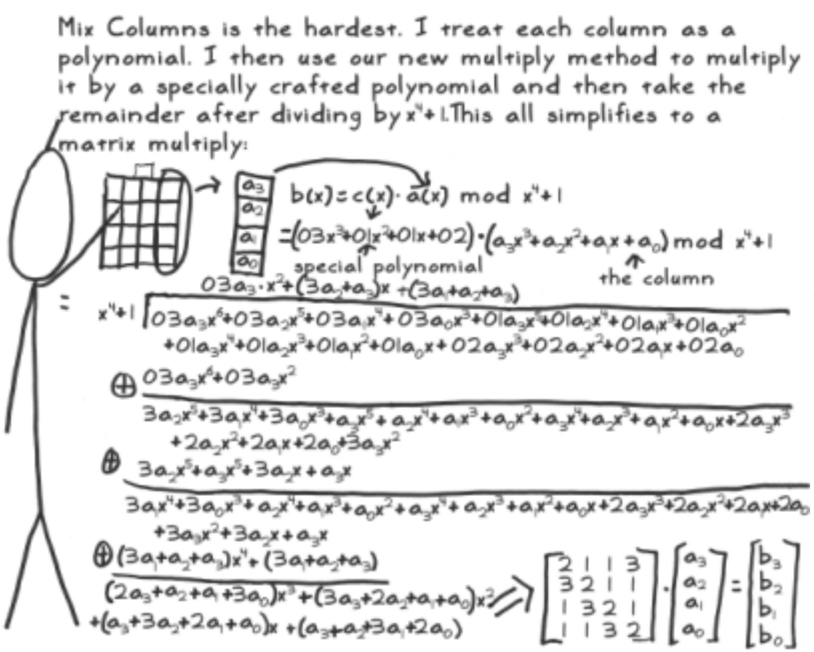
- Key size
  - 56 bits, 2^{56} = 72,057,594,037,927,936
- DES Challenges
  - Sponsored by RSA Security
  - Challenge I: 96 days
  - Challenge II: 41 days, distributed.net
  - Challenge II-2: 56 hours, EFF deep crack
    - $250,000 to develop, $10,000 prize
    - 90 billion keys/second
  - Challenge III: 22 hours, EFF/distributed.net
  - 2008, FPGA, 1 day

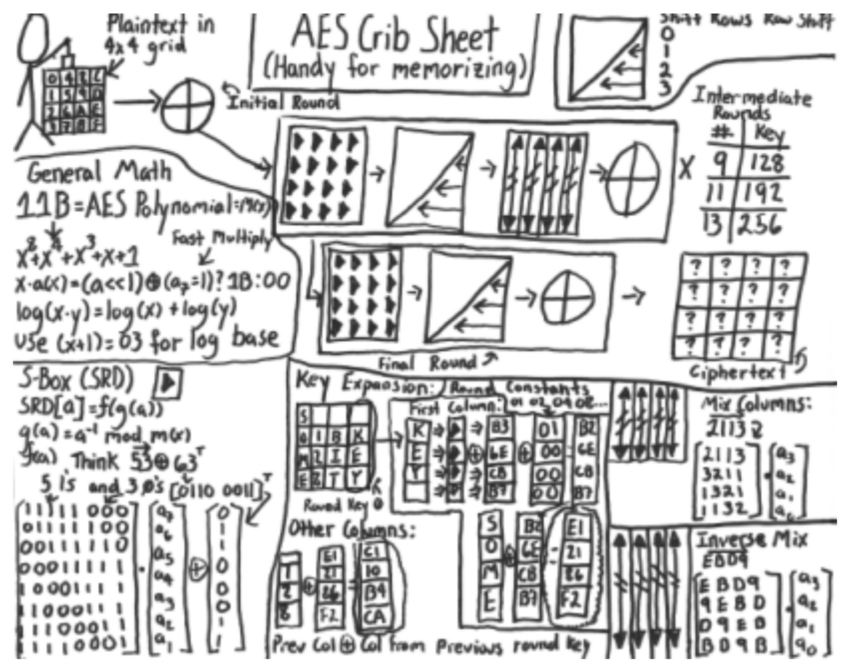
Stronger symmetric schemes

- 3DES
  - Use DES to encrypt with one key
  - Decrypt with a second key
  - Encrypt with a third key
  - 168-bits instead of 56-bits
  - Advantages:
    - Uses DES, most analyzed algorithm
    - No known effective attack besides brute-force
  - Disadvantages:
    - Slow in software, DES designed for 1970's hardware
    - Small block size of 64-bits

AES

- Advanced Encryption Standard (AES)
  - 2001 new NIST standard, Rijndael
  - Symmetric block cipher
  - Key lengths of 128, 192, and 256 bits
  - Approved by NSA for top secret information

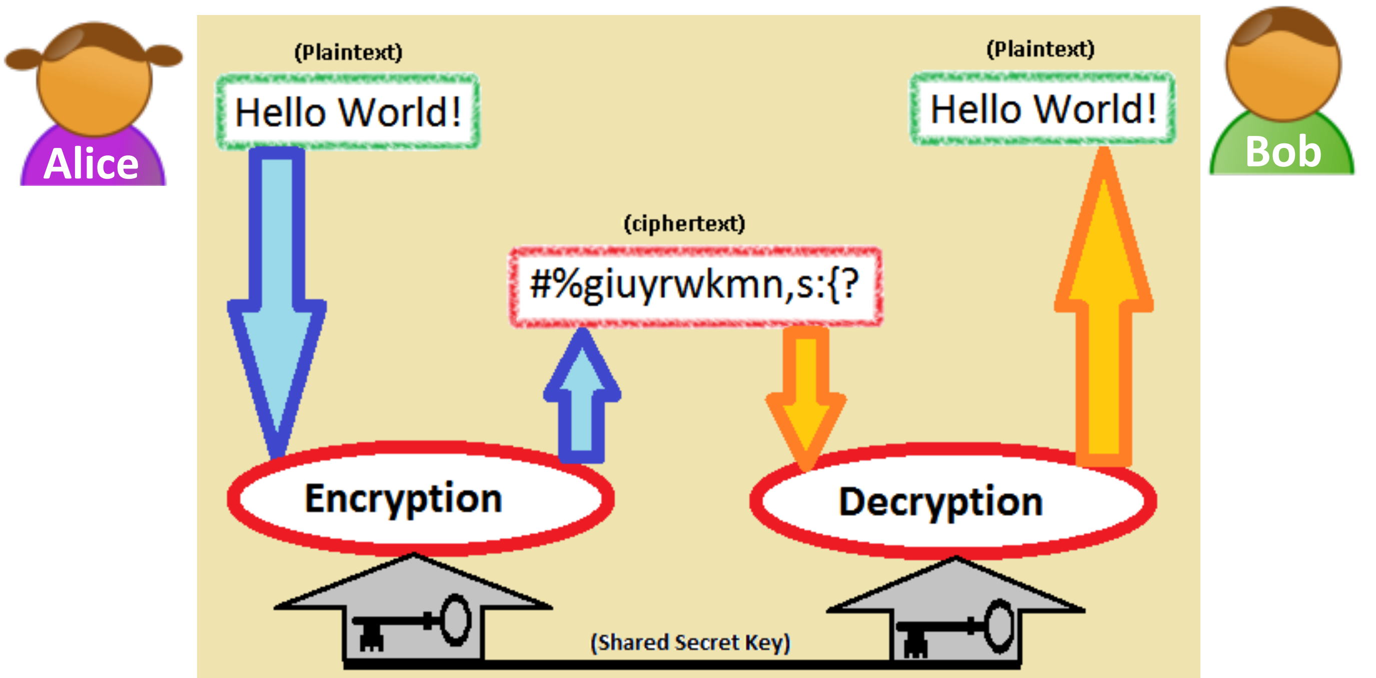




http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

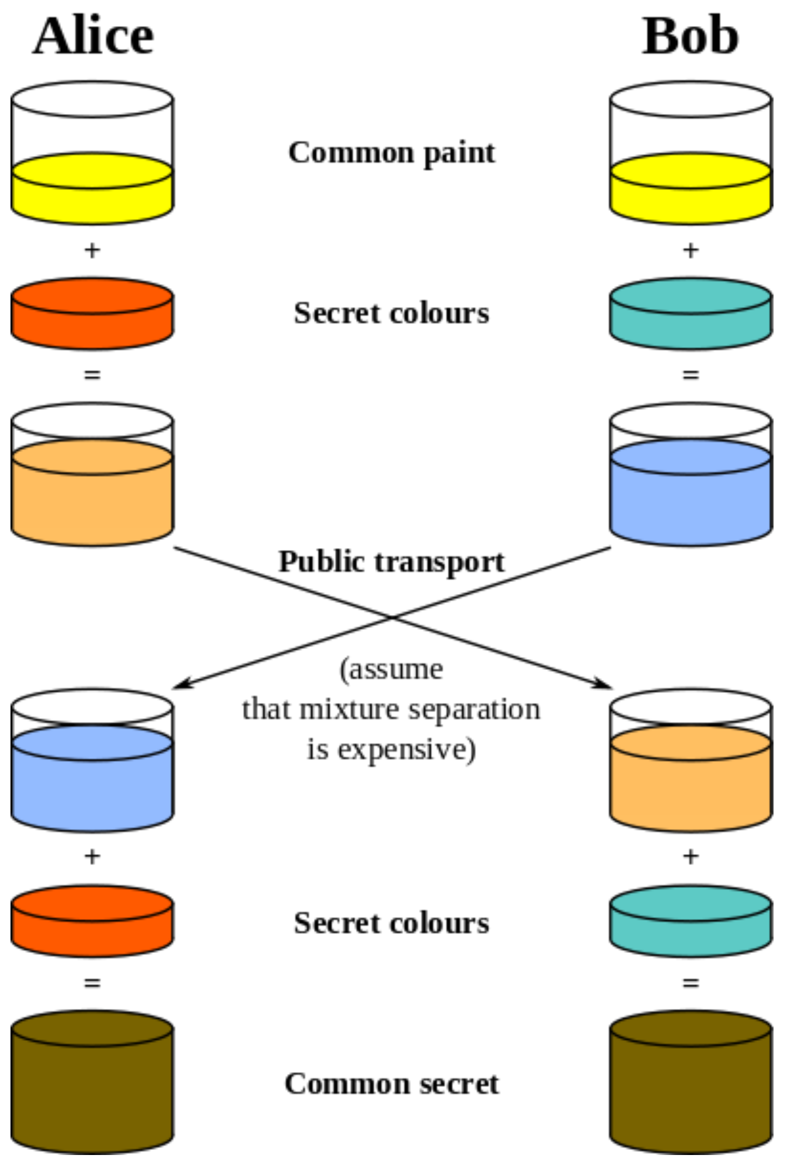
Key exchange

- Thus far: symmetric encryption
  - Alice and Bob need to have shared secret
  - But how do you distribute?
  - Doesn't scale



Diffie-Hellman

- Diffie-Helman (DH) key exchange
  - 1976, Whitfield Diffie & Martin Hellman
  - Alice and Bob agree on a private secret:
    - On a public channel
    - Where Eve hears all the traffic
    - Only Alice and Bob end up knowing the secret
  - Relies on one-way function
    - Easy to do but difficult to undo



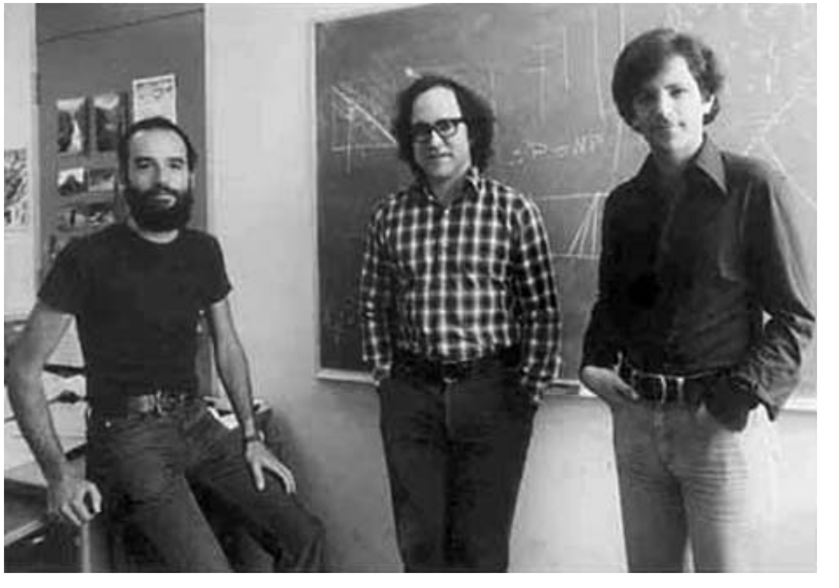
Alice	Bob
Alice and Bob agree on values for Y and P for the one-way function Y^x (mod P), e.g. Y=7, P=11	
Alice chooses secret number A = 3	Alice chooses secret number B = 6
$\alpha = 7^A \pmod{11}$ $= 7^3 \pmod{11}$ $= 2$	$\beta = 7^B \pmod{11}$ $= 7^6 \pmod{11}$ $= 4$
Sends α = 2 to Bob	Sends β = 4 to Alice
Using Bob's result: $\beta^A \pmod{11}$ $4^3 \pmod{11} =$ **9**	Using Alice's result $\alpha^B \pmod{11}$ $2^6 \pmod{11} =$ **9**

Public key cryptography

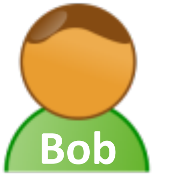
- Diffie-Helman key exchange
  - Both parties had to be around to negotiate secret
- Symmetric encryption
  - Encrypting message M with key K: $E_k(M) = C$
  - Decrypting ciphertext C with key K: $D_K(C) = M$
- Asymmetric encryption
  - 1975, Diffie conceives of idea
  - Users have a private key and a public key
    - Alice encrypts plaintext with Bob's public key
    - Only Bob can (tractably) decrypt using his private key
  - Special one-way function
    - Hard to reverse unless you know something special

RSA

- RSA public key encryption
  - 1977, Rivest, Shamir, Adlerman
  - Choose two prime numbers, p and q
    - Public key: N = pq
    - Private key: p and q
    - Factoring N that is produced by two large primes is hard

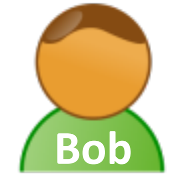


RSA example



Alice	Bob
Alice picks two giant primes, p and q e.g. p = 61, q = 53 N = p * q = 61 * 53 = 3233 (p – 1) * (q- 1) = 60 * 52 = 3120 Find number 1< e < 3120, e is relatively prime with 3120, say e = 17 **Alice's public key: N = 3233, e = 17**	
	Bob wants to send message 65 to Alice, looks up her public key. $C = M^e \pmod{N}$ $C = 65^{17} \pmod{3233} = 2790$

RSA example



Alice	Bob
	Bob wants to send message 65 to Alice, looks up her public key. $C = M^e \pmod N$ $C = 65^{17} \pmod{3233} = 2790$
Compute special number d $e * d = 1 \pmod{(p-1) * (q-1)}$ $17 * d = 1 \pmod{3120}$ d = 2753 (using Euclid's algorithm) **Alice's private key d = 2753, or p and q** Decrypt message: $M = C^d \pmod N$ $M = 2790^{2753} \pmod{3233} = 65$	

RSA security

- Attacks on RSA
  - Brute force
    - Try all possible private keys
    - Use a large key space, but slows things down
    - RSA is not as fast as symmetric crypto
  - Mathematical
    - Factoring the product of two large primes
  - Timing
    - Keep track of how long it takes to decipher messages
  - Chosen ciphertext

$$O\left(\exp\left(\left(\frac{64}{9}b\right)^{\frac{1}{3}}(\log b)^{\frac{2}{3}}\right)\right)$$

2009
768-bit RSA factored using
hundreds of machines in 2 years

Unsolved problems in computer science

Can integer factorization be done in polynomial time?

Summary

- Historical cryptography
  - Code talkers
- Modern cryptography
  - Computer-based symmetric ciphers
    - DES, 3DES, AES
  - Rise of asymmetric cryptography
    - Diffie-Hellman
    - RSA