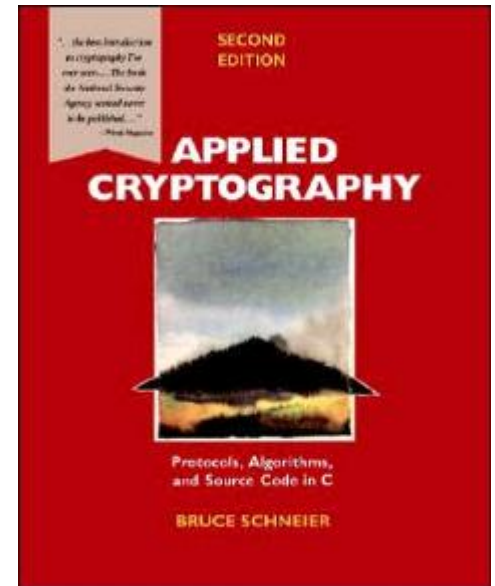
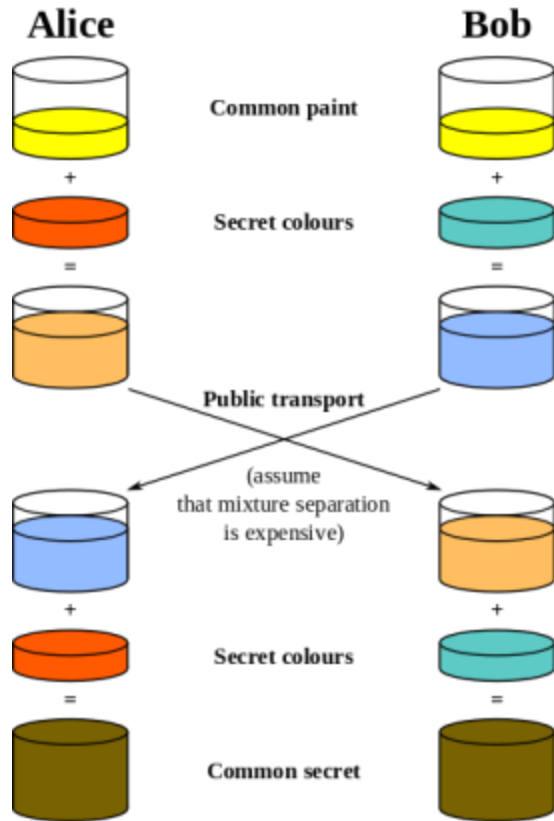


Modern Cryptography

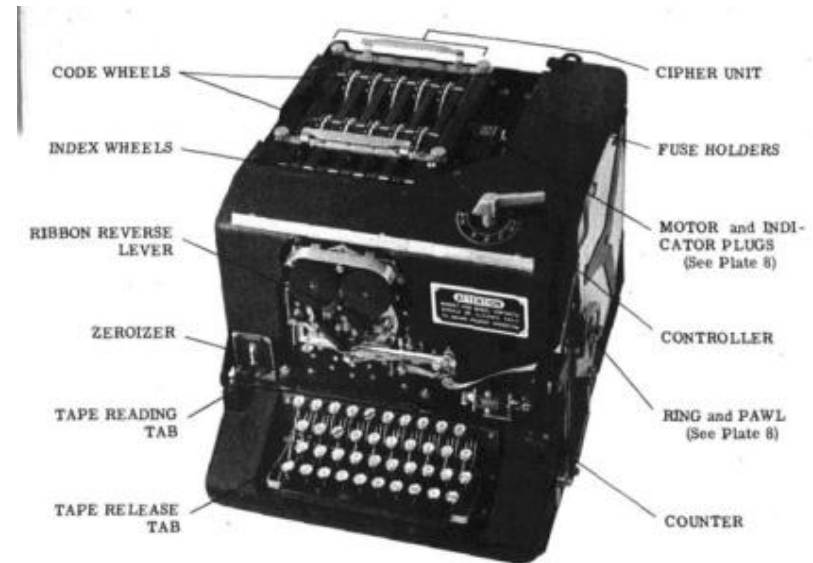


Overview

- 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 (SIGABA)**
 - United States
 - 15 rotors
 - No known successful cryptanalysis during service lifetime
 - But big, expensive, fragile



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

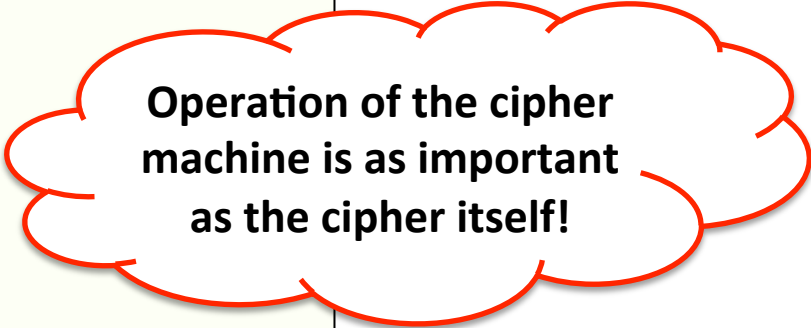
Failing to use system of narrowest distribution

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 outsiders had learned the unwritten language
 - 3 line message, 20 s vs. machine 30 min
 - Lexicon of 274 words + phonetic alphabet



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

Modern cryptography

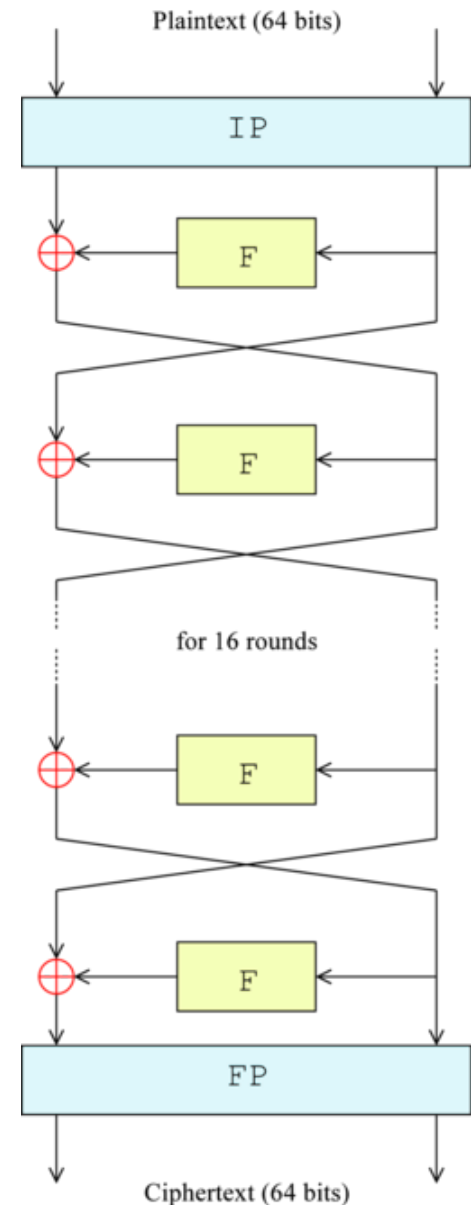
- Moving into computer age
 - Not limited to physical engineering constraints
 - 100's of rotors instead of 3, changing in complex ways
 - Much faster
 - Scrambling at the bit level
- Symmetric encryption (what we've seen thus far)
 - Encrypting message M with key K : $E_K(M) = C$
 - Decrypting ciphertext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

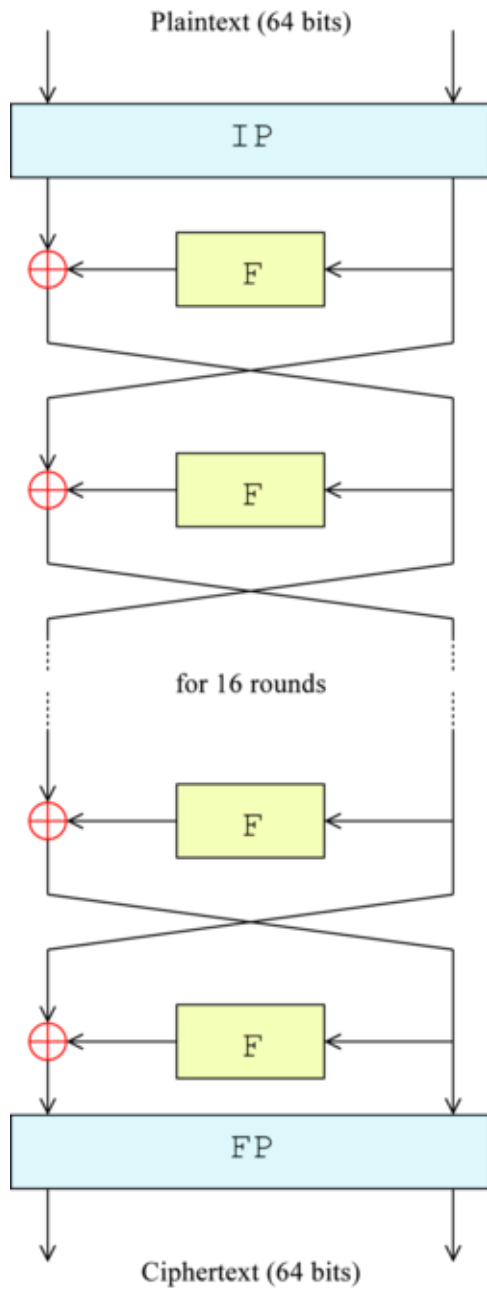
DES

- Data Encryption Standard (DES)
 - NIST wanted a government 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

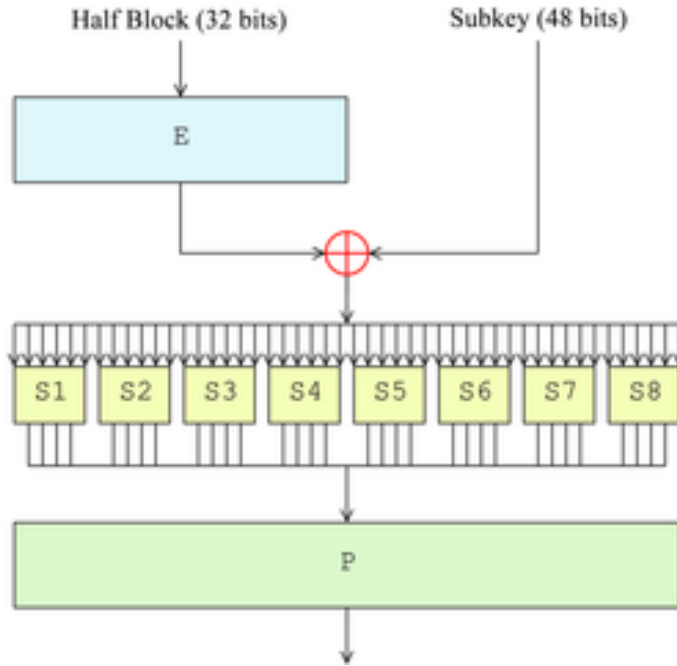
"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure"

-Bruce Schneier

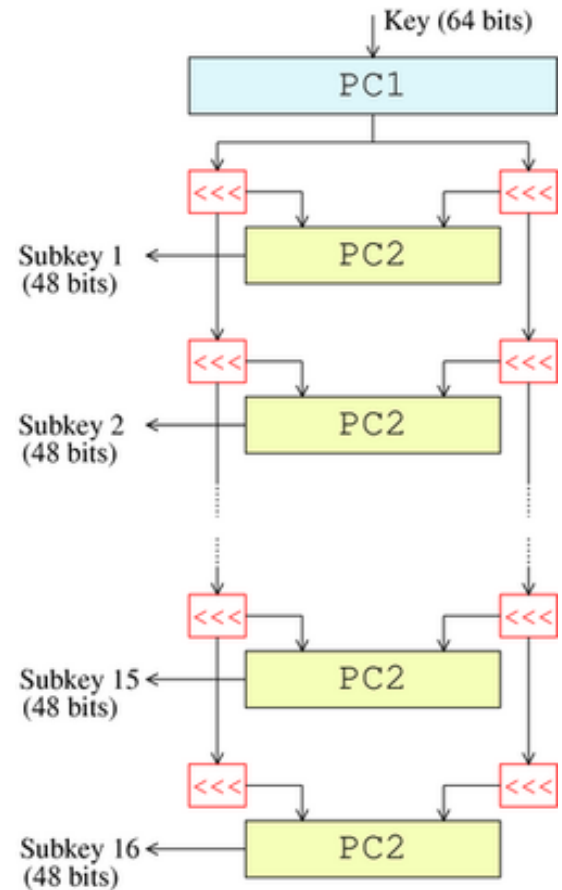




Overall structure



The Feistel function (F-function)



Key schedule

Breaking DES

- Key size, 72 quadrillion
 - 56 bits, $2^{56} = 72,057,594,037,927,936$
- DES Challenges (brute force attacks)
 - Sponsored by RSA Security
 - Challenge I: 96 days, Internet users
 - 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

- Triple DES (3DES)

- ciphertext: $E_{K_3}(D_{K_2}(E_{K_1}(\text{plaintext})))$

- plaintext: $D_{K_1}(E_{K_2}(D_{K_3}(\text{ciphertext})))$

- Keying option 1: $K_1 \neq K_2 \neq K_3$

- 168-bits instead of 56-bits

- Advantages:

- Uses DES, most analyzed crypto 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

Mix Columns is the hardest. I treat each column as a polynomial. I then use our new multiply method to multiply it by a specially crafted polynomial and then take the remainder after dividing by x^4+1 . This all simplifies to a matrix multiply:



$$b(x) = c(x) \cdot \bar{a}(x) \pmod{x^4+1}$$

$$= (03x^3 + 01x^2 + 01x + 02) \cdot (a_3x^3 + a_2x^2 + a_1x + a_0) \pmod{x^4+1}$$

special polynomial the column

$$= \frac{03a_3x^6 + 03a_2x^5 + 03a_1x^4 + 03a_0x^3 + 01a_3x^5 + 01a_2x^4 + 01a_1x^3 + 01a_0x^2 + 01a_3x^4 + 01a_2x^3 + 01a_1x^2 + 01a_0x + 02a_3x^3 + 02a_2x^2 + 02a_1x + 02a_0}{x^4+1}$$

$$\oplus \frac{03a_3x^2 + 03a_2x^3}{3a_2x^3 + 3a_1x^2 + 3a_0x + a_3x^3 + a_2x^2 + a_1x + a_0x^3 + a_2x^2 + a_1x + a_0x^2 + 2a_3x^3 + 2a_2x^2 + 2a_1x + 2a_0}$$

$$\oplus \frac{3a_2x^3 + a_3x^2 + 3a_1x + a_0x}{3a_1x^3 + 3a_0x^2 + a_2x^3 + a_1x^2 + a_0x^3 + a_2x^2 + a_1x^2 + a_0x^2 + 2a_3x^2 + 2a_2x^2 + 2a_1x + 2a_0}$$

$$\oplus \frac{(3a_1 + a_2 + a_3)x^3 + (3a_0 + a_1 + a_2)x^2}{(2a_3 + a_2 + a_1 + 3a_0)x^3 + (3a_2 + 2a_1 + a_0)x^2 + (a_3 + 3a_1 + 2a_0)x + (a_2 + a_3 + 3a_0 + 2a_0)}$$

$$\Rightarrow \begin{bmatrix} 2 & 1 & 1 & 3 \\ 3 & 2 & 1 & 1 \\ 1 & 3 & 2 & 1 \\ 1 & 1 & 3 & 2 \end{bmatrix} \cdot \begin{bmatrix} a_3 \\ a_2 \\ a_1 \\ a_0 \end{bmatrix} = \begin{bmatrix} b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix}$$

Plaintext in 4x4 grid

AES Crib Sheet (Handy for memorizing)

Initial Round

General Math

1.9B = AES Polynomial: $x^4 + x^3 + x^2 + x + 1$

Fast Multiply

$x \cdot ax = (a \ll 1) \oplus (a_2 = 1) ? 1B : 00$

$\log(x \cdot y) = \log(x) + \log(y)$

Use $(x+1) = 03$ for log base

S-Box (SRD)

$SRD[a] = f(g(a))$

$g(a) = a^{-1} \pmod{m(x)}$

5 is and 3 is $(0110\ 0011)^T$

Key Expansion: 1 Round Constants

First Column: $01\ 02\ 04\ 08\ \dots$

Other Columns:

Mix Columns: $2113\ 2$

Inverse Mix: $E0B4$

Ciphertext

Intermediate Rounds

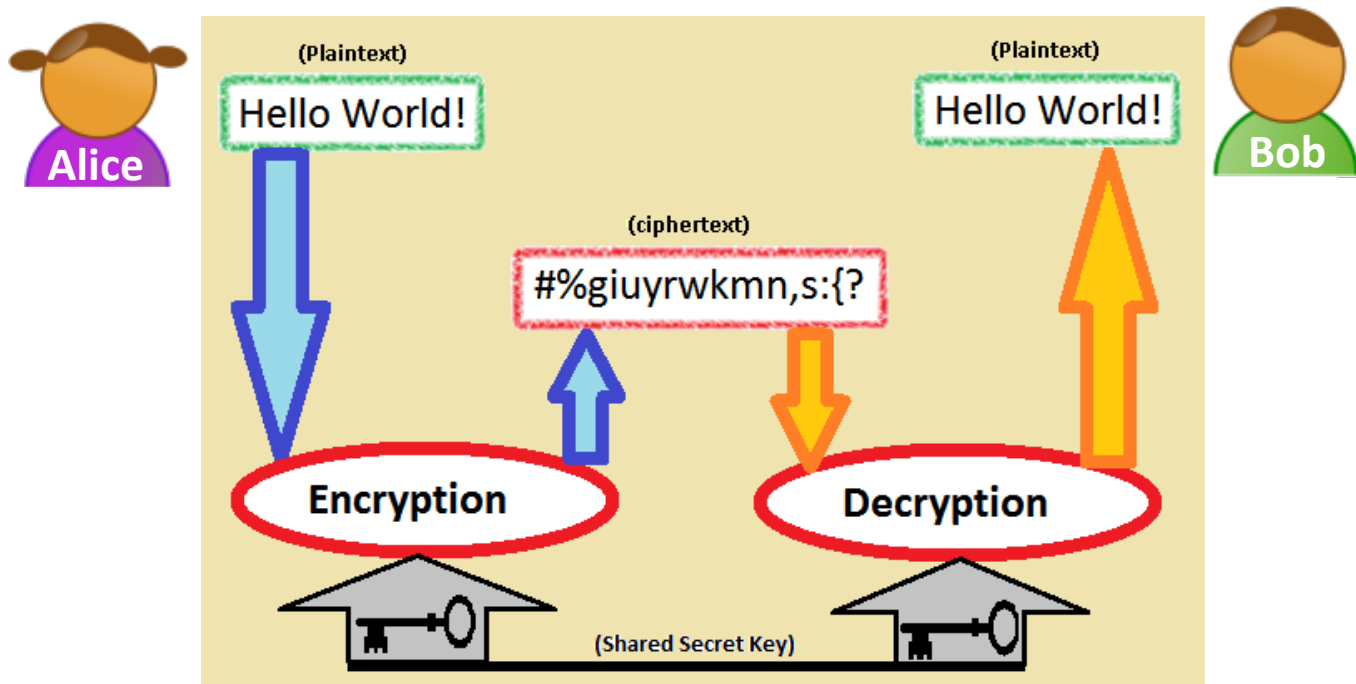
#	Key
9	128
11	192
13	256

Final Round

Prev Col @ Col from Previous round Key

Key exchange

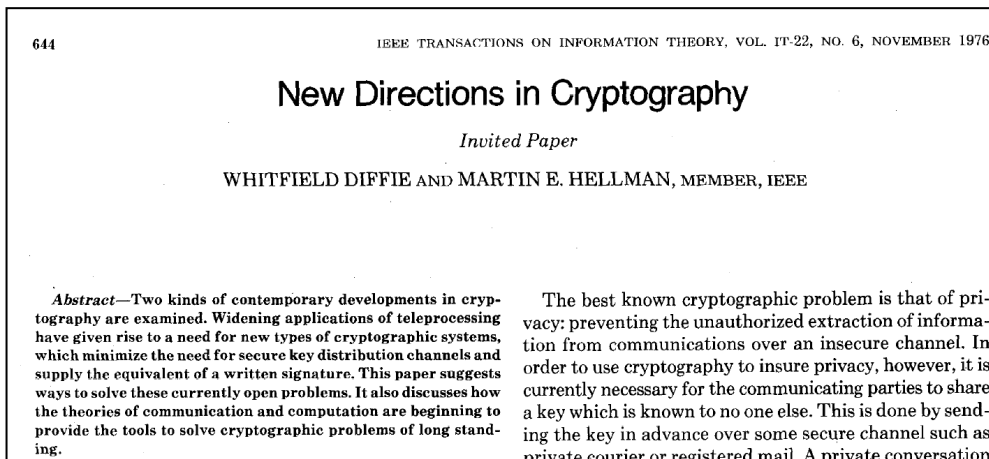
- Thus far: **symmetric encryption**
 - Alice and Bob need to have shared secret
 - But how do you distribute?
 - Doesn't scale



Diffie-Hellman

- Diffie-Hellman (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**
 - Function that is easy to do, but difficult to undo

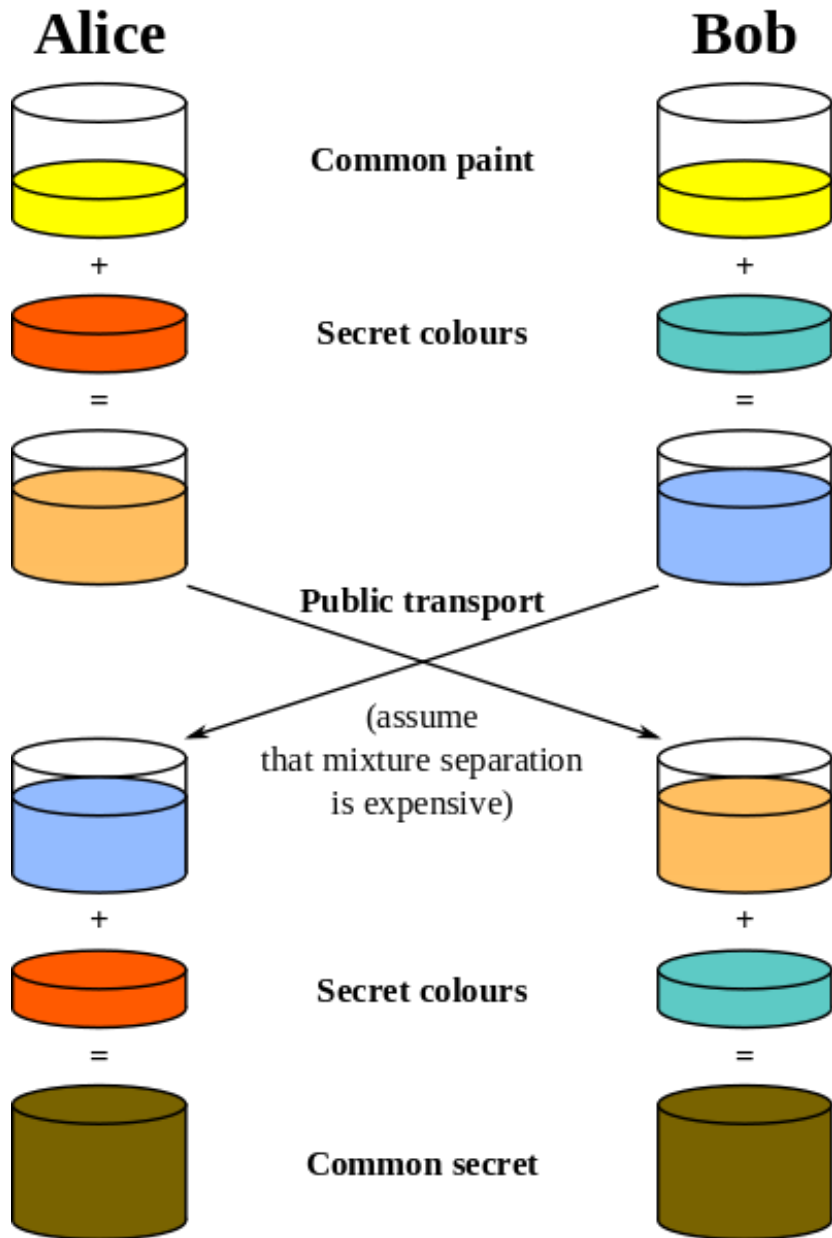
<http://www.youtube.com/watch?v=3QnD2c4Xovk>



Whitfield Diffie



Martin Hellman



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

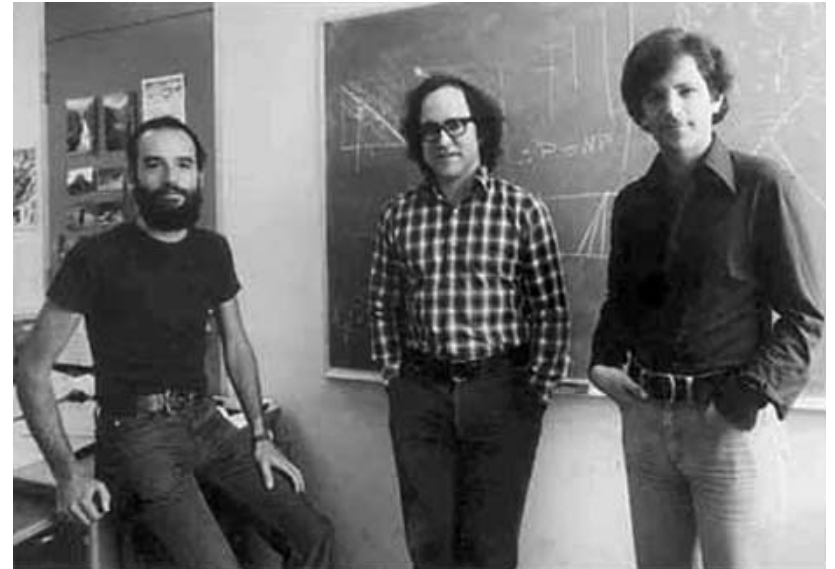
Public key cryptography

- **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, Adleman
 - Choose two prime numbers, p and q
 - Public key: $N = pq$
 - Private key: p and q
 - Factoring N if N is product of two large primes is "hard"

http://www.youtube.com/watch?v=wXB-V_Keiu8



RSA example



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

RSA example



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

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

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

- Mathematical

- Factoring the product of two large primes

- Timing

- Keep track of how long it takes to decipher messages

- Chosen ciphertext

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