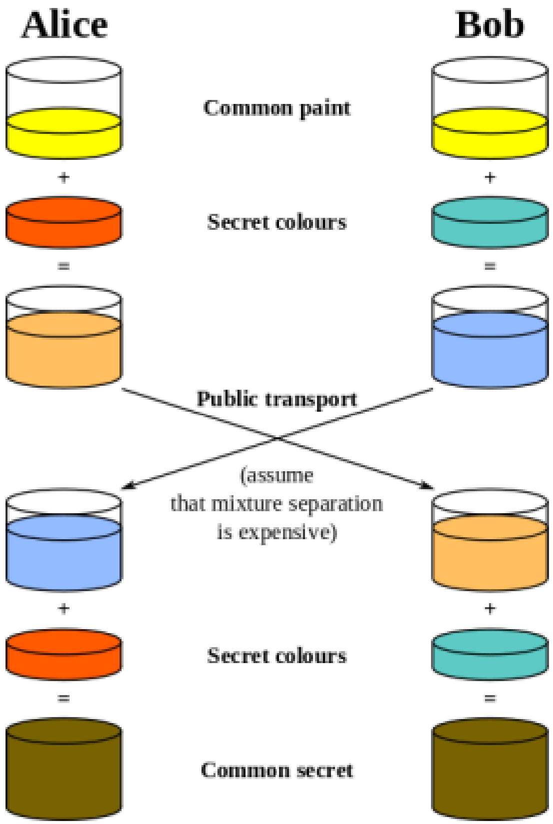
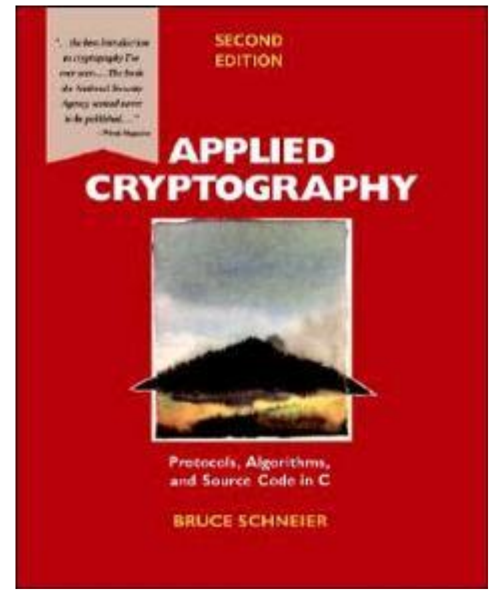
Modern cryptography





Overview

- Modern cryptography
  - Symmetric cryptography
    - DES
    - 3DES
    - AES
  - Asymmetric cryptography
    - Diffie-Hellman key exchange

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: operates one bit/byte at-a-time
  - Block cipher: operates on a group of bits/bytes

Bit encryption / decryption example

```
Message         : HELLO
```

Sender

```
Binary          : 1001000 1000101 1001100 1001100 1001111
KEY = DAVID     : 1000100 1000001 1010110 1001001 1000100
Encrypted (XOR) : 0001100 0000100 0011010 0000101 0001011
```

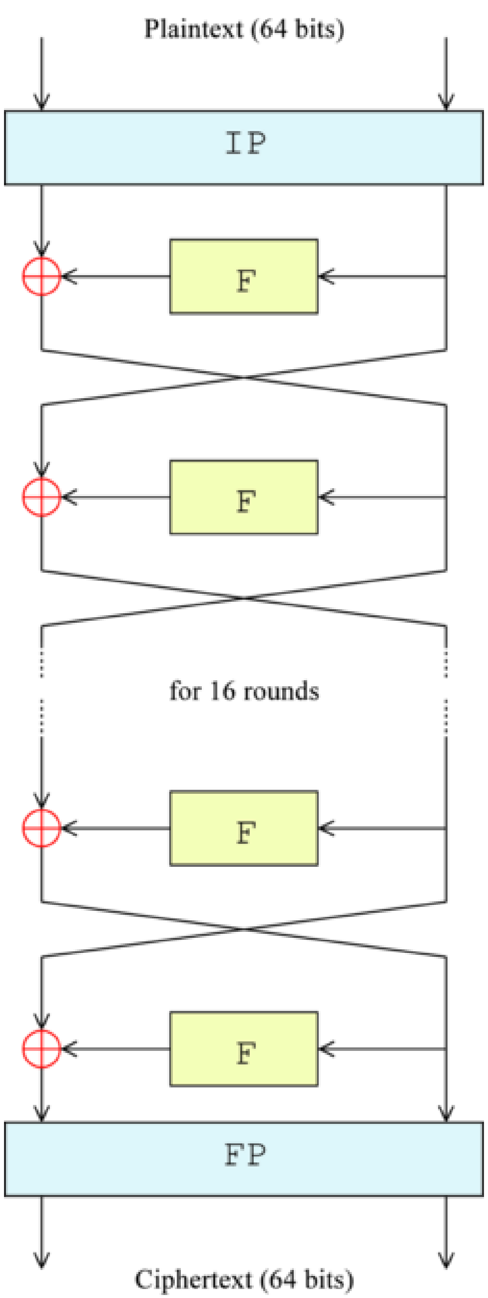
Receiver

```
Encrypted       : 0001100 0000100 0011010 0000101 0001011
KEY = DAVID     : 1000100 1000001 1010110 1001001 1000100
Decrypted (XOR) : 1001000 1000101 1001100 1001100 1001111
```

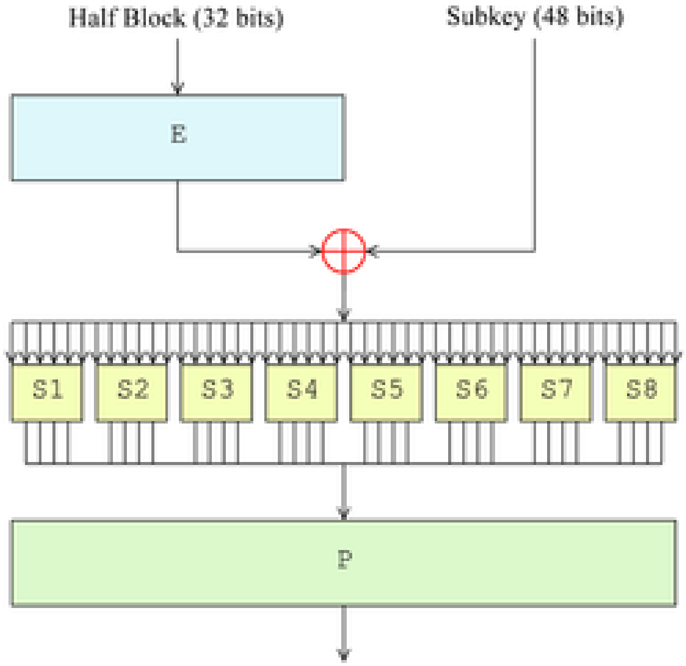
DES

- Data Encryption Standard (DES)
  - NIST wanted a government standard
  - Based on IBM's Lucifer cipher
    - 16 round Feistel network
    - Security provided by a key
    - With "cooperation" from NSA:
      - Improved S-boxes
      - Reduced key length to 56 bits
  - 1976 approved as a standard
  - Same hardware/software can encrypt/decrypt

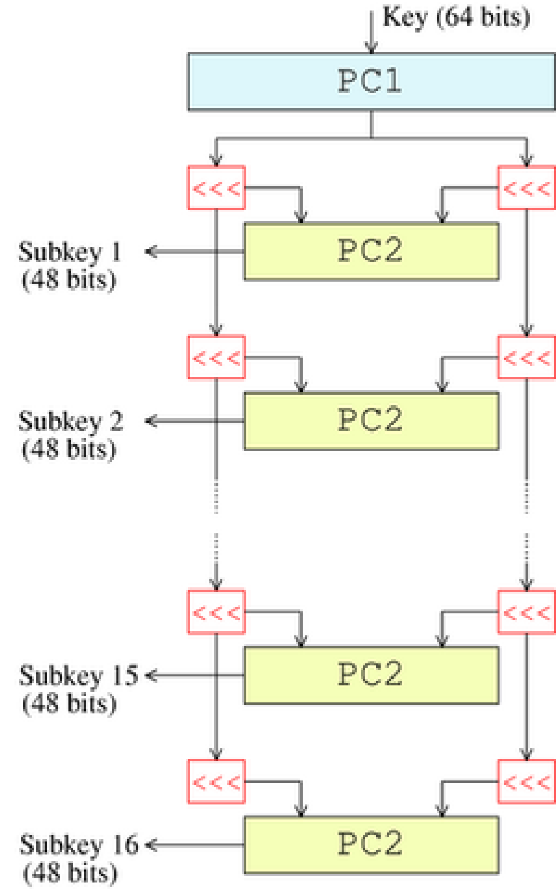
> *"DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study: one that the NSA said was secure"*
>
> *-Bruce Schneier*



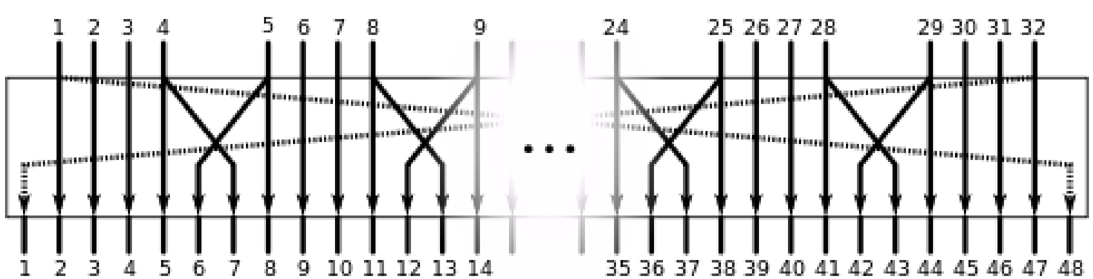
Overall structure



The Feistel function (F-function)



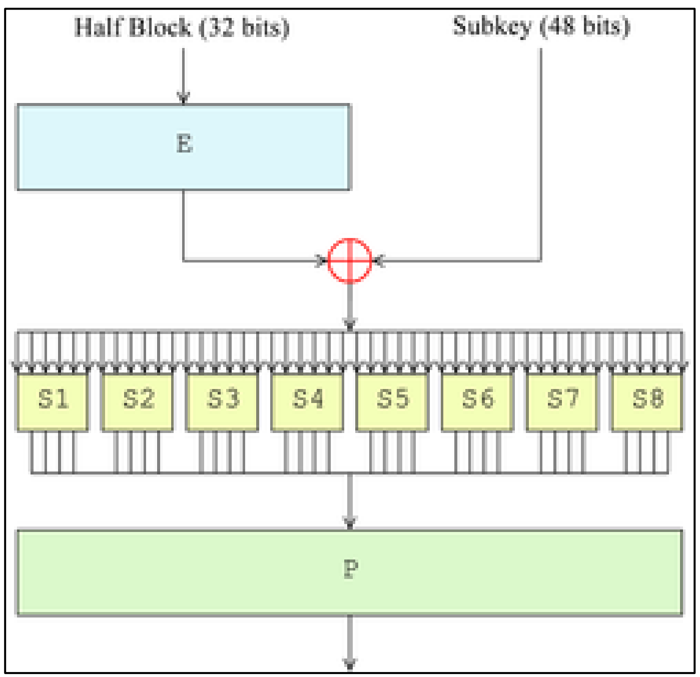
Key schedule



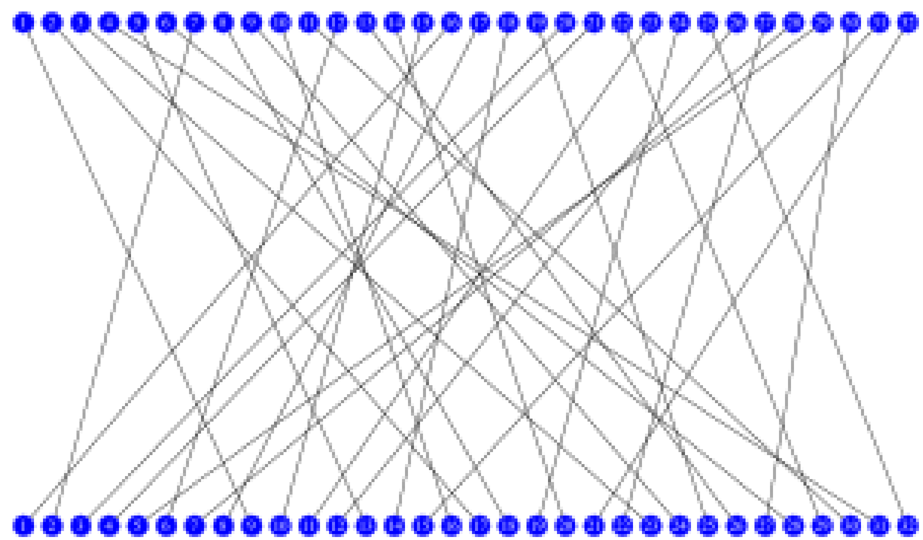
E-box, expansion permutation, 32 -> 48 bits

S_5																
	x0000x	x0001x	x0010x	x0011x	x0100x	x0101x	x0110x	x0111x	x1000x	x1001x	x1010x	x1011x	x1100x	x1101x	x1110x	x1111x
0yyyy0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
0yyyy1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
1yyyy0	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
1yyyy1	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S-box #5, 6 bits -> 4 bits, e.g. 011011 -> 1001 (9)



The Feistel function (F-function)



P-box, straight permutation, 32 bits -> 32 bits

Breaking DES

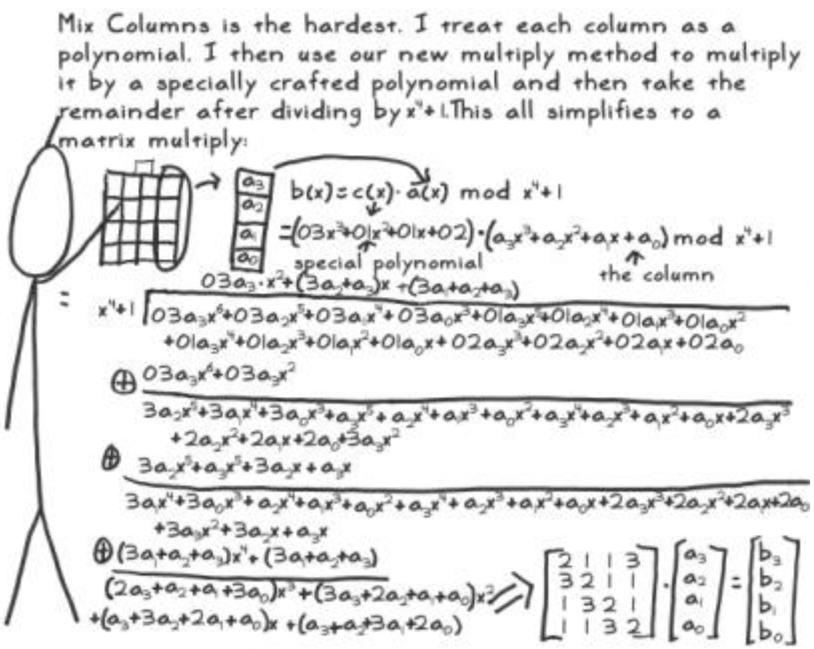
- Key size, 72 quadrillion
  - 2^{56} = 72,057,594,037,927,936
- DES Challenges (brute force)
  - Sponsored by RSA Security
    - Challenge I: 96 days, Internet users
    - Challenge II: 41 days, distributed.net
    - Challenge II-2: 56 hours, EFF deep crack
      - \$250,000 to develop, \$10,000 prize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

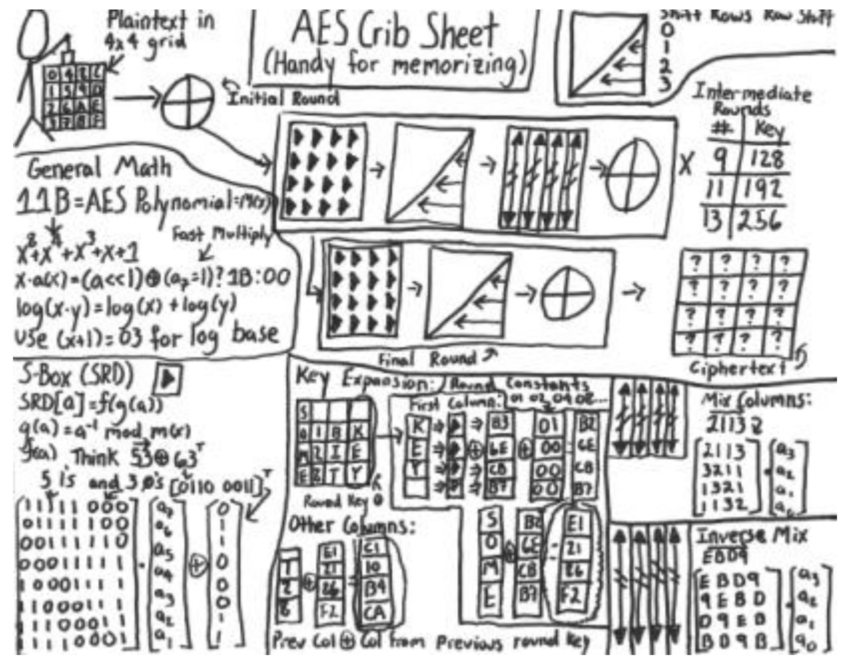
Stronger symmetric schemes

- Triple DES (3DES)
  - Ciphertext: $E_{K3}(D_{K2}(E_{K1}(\texttt{plaintext})))$
  - Plaintext: $D_{K1}(E_{K2}(D_{K3}(\texttt{ciphertext})))$
  - Keying option 1: K1 ≠ K2 ≠ K3
    - 168 bits = 56 bits x 3
  - Advantages:
    - Uses DES, most analyzed encryption 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





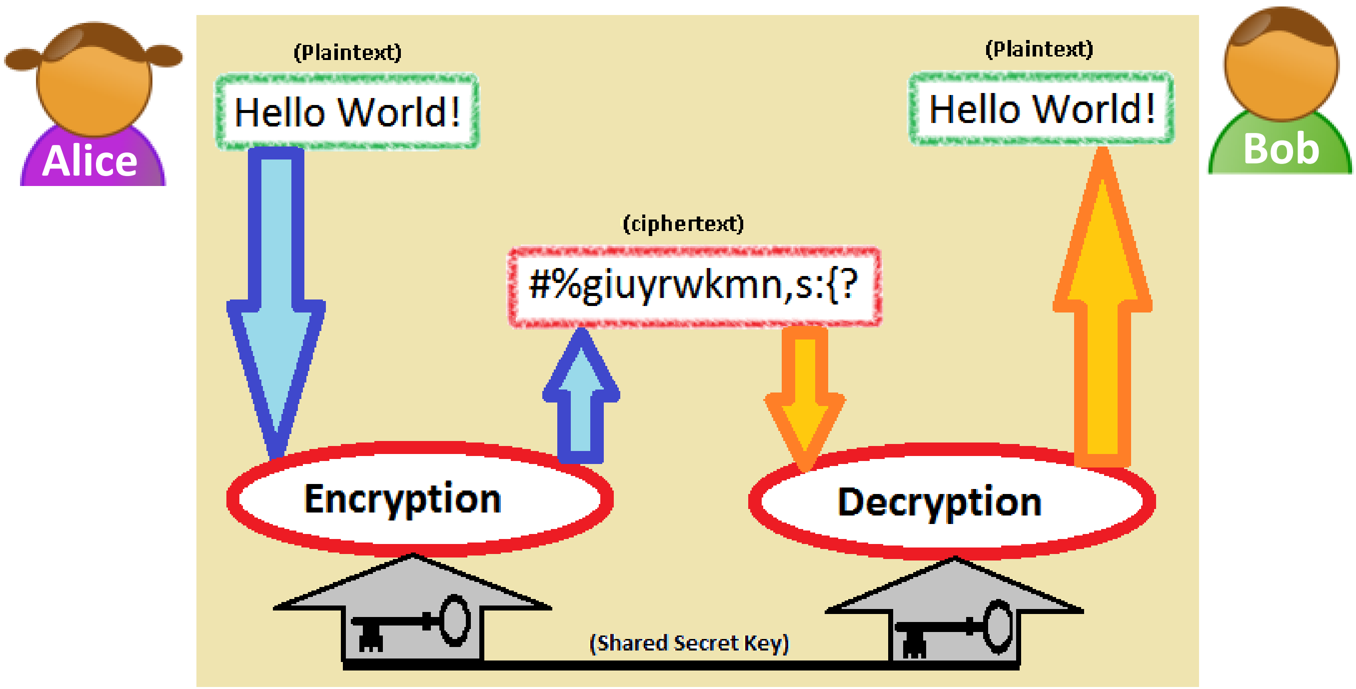
http://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html

Attack types

- Ciphertext only
  - Ciphertext of message(s), plaintext unknown
- Known plaintext
  - Ciphertext plus corresponding plaintext
- Chosen plaintext
  - Ciphertext plus plaintext of your own choosing
  - Adaptive chosen plaintext
    - Modify plaintext based on previous decryptions
- Rubber hose
- …

Key exchange

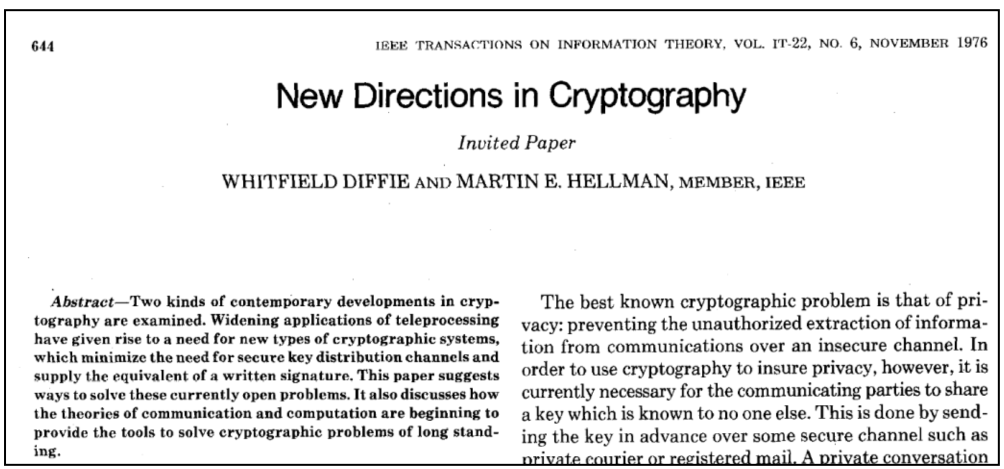
- Thus far: symmetric encryption
  - Alice and Bob need to have shared secret
  - But how do you distribute?
  - Doesn't scale



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 must be easy to do, but difficult to undo

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



644 IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

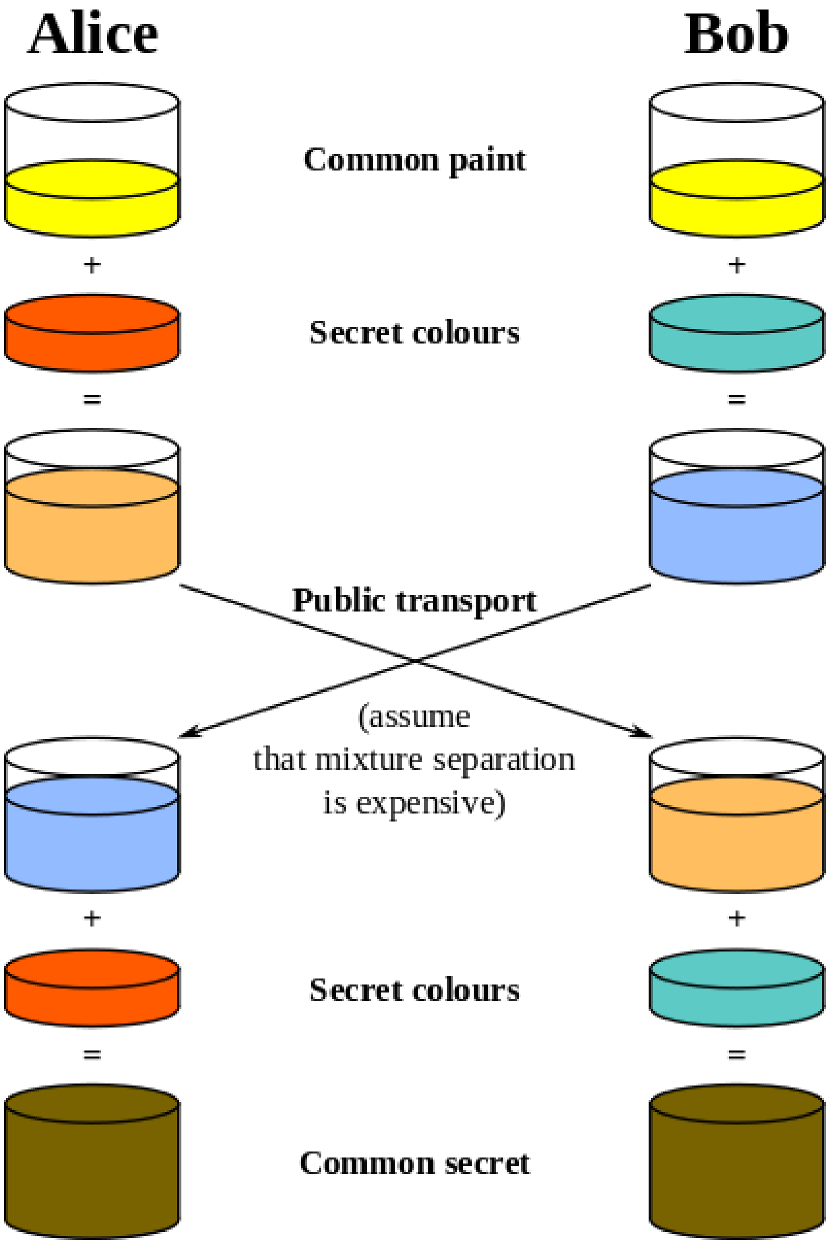
WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

Abstract—Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

The best known cryptographic problem is that of privacy: preventing the unauthorized extraction of information from communications over an insecure channel. In order to use cryptography to insure privacy, however, it is currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such as private courier or registered mail. A private conversation

Whitfield Diffie

Martin Hellman



Alice	Bob
Alice and Bob agree publicly 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: $B = 6$
$\alpha = 7^A \pmod{11}$ $= 7^3 \pmod{11}$ $= 343 \pmod{11}$ $= 2$	$\beta = 7^B \pmod{11}$ $= 7^6 \pmod{11}$ $= 117649 \pmod{11}$ $= 4$
Sends $\alpha = 2$ to Bob	Sends $\beta = 4$ to Alice
Using Bob's result: $\beta^A \pmod{11}$ $4^3 \pmod{11} = 9$ $7^{B*A} \pmod{11}$	Using Alice's result $\alpha^B \pmod{11}$ $2^6 \pmod{11} = 9$ $7^{A*B} \pmod{11}$

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

Summary

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