601.445/645
Practical Cryptographic Systems

Symmetric Cryptography II

Instructor: Matthew Green

Housekeeping

- Waitlist: I promise that if you stick it out you will get into the class
- **Assignment 1: out last Friday! (Check Piazza!)**
  - The Gradescope for submission will be up in a day or two, please hang in there!
- **My office hours: 1-2:45pm Malone 313 or 309**
- **TA office hours: 5:30-6:30 Mondays, Malone 216**

News

News

Meet Willow, our state-of-the-art quantum chip

Dec 09, 2024
6 min read

Our new chip demonstrates error correction and performance that paves the way to a useful, large-scale quantum computer

Hartmut Neven
Founder and Lead, Google Quantum AI

Read AI-generated summary

Share

Review

- Last time: classical cryptography:

  Shift cipher
  Substitution cipher
  Vigenere cipher
  One-time ciphers

- Today:

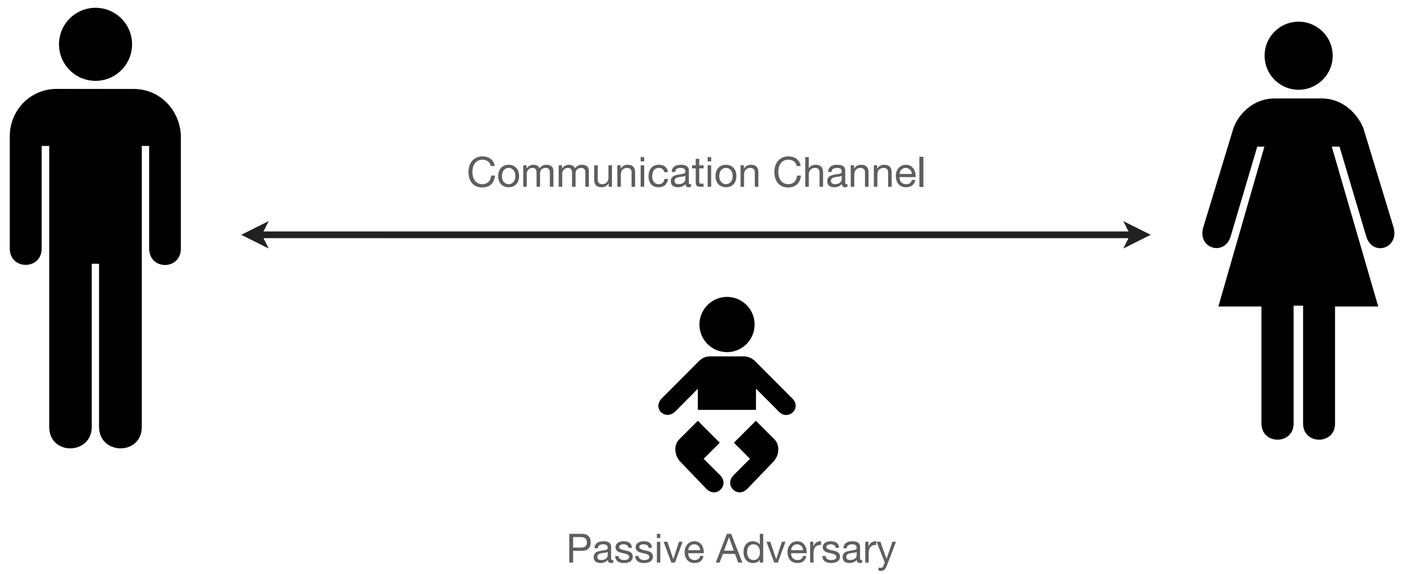
  - Mechanical cryptography, towards block ciphers

Ideas we introduced

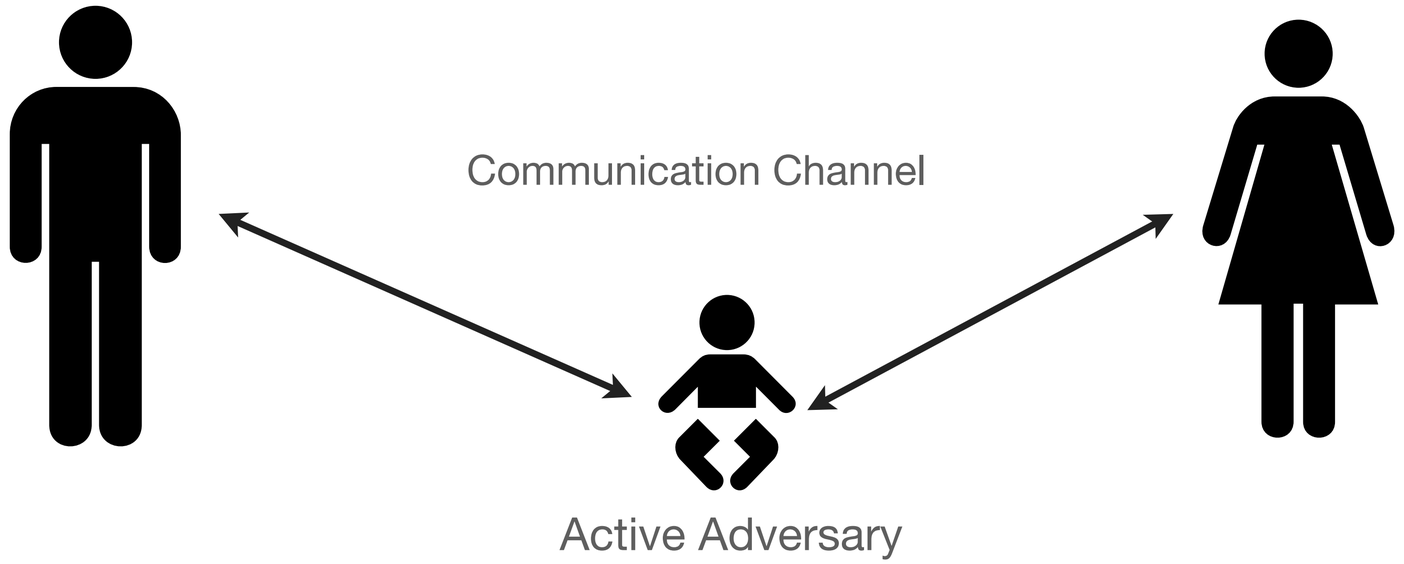
- Communication channels and adversaries
- Notions of confidentiality and authenticity
- Tools:
  - Ciphers and encipherment, MACs, Digital signatures
- One-time ciphers
  - “Shannon secrecy”

Communication Model

Communication Model



Communication Model



Secure Communication

- Two basic properties we like to achieve:
  - Data confidentiality
  - Data authenticity (“integrity”)
- Tools:
  - Encryption
  - Message Authentication Codes (MACs)
  - Digital Signatures

Ciphers

- A cipher is a “scheme” and consists of three algorithms:
  - **KeyGen**() -> *key*
    Enc(*key, plaintext*) -> ciphertext
    Dec(*key, ciphertext*) -> plaintext

    (all algorithms may use randomness!)
- We will also use these terms:

  Keyspace (set of all possible keys)
  Message space (set of all possible messages)
  Ciphertext space (set of all possible ciphertexts

Ciphers

- Scheme should be “correct”:

Ciphers

- Scheme should be “correct”:

  For all keys: *key* <- **KeyGen**()
  it should hold that **Dec**(*key,* **Enc(***key, m*)) == *m* for all allowed m

Ciphers

- Scheme should be “correct”:

  For all keys: *key* <- **KeyGen**()
  it should hold that **Dec**(*key*, **Enc(***key*, *m*)) == *m* for all allowed m

- Scheme should probably be secure too!
  - But what in the world does “secure” mean?

Security for ciphers

- Some ideas:
  - “Hide the key” (attacker cannot recover key)

Security for ciphers

- Some ideas:
  - “Hide the key” (attacker cannot recover key)
  - “Hide the message” (attacker cannot recover the plaintext)

Security for ciphers

- Some ideas:
  - “Hide the key” (attacker cannot recover key)
  - “Hide the message” (attacker cannot recover the plaintext)
  - “Hide all information possible”
    (attacker learns nothing but the length of the message,
    and any information they had about the message before seeing the ciphertext.)

Security for ciphers

- Some ideas:
  - “Hide the key” (attacker cannot recover key)
  - “Hide the message” (attacker cannot recover the plaintext)
  - “Hide all information possible”
    (attacker learns nothing but the length of the message,
    and any information they had about the message before seeing the ciphertext.)

Shannon secrecy

- Let *D* be some distribution over the plaintext space
  (this is what the adversary knows about the messages before seeing a ciphertext!)
- Attacker now sees a ciphertext *C*
- How do we characterize the attacker's knowledge about the plaintext?

  $D \mid C$

- Shannon secrecy holds if *D* and $(D \mid C)$ are identical

Security for ciphers

Definition (Shannon Secrecy)

A cipher $(\mathcal{M}, \mathcal{K}, \mathsf{KG}, \mathsf{Enc}, \mathsf{Dec})$ is **Shannon secure w.r.t a distribution** D over $\mathcal{M}$ if for all $m' \in \mathcal{M}$ and for all c,

$$\Pr\left[m \leftarrow D : m = m'\right] = \Pr\left[k \leftarrow \mathsf{KG}, m \leftarrow D : m = m' | \mathsf{Enc}(m, k) = c\right]$$

From: https://www3.cs.stonybrook.edu/~omkant/s18/L02-s18.pdf

Vigenere

S	E	N	D	R	E	I	N	F	O	R	C	E	M	E	N	T	S
V	I	G	E	N	E	R	E	V	I	G	E	N	E	R	E	V	I
N	M	T	H	E	I	Z	R	A	W	X	G	R	Q	V	R	O	A

One-Time Ciphers

- 1900s
  - Vernam & Mauborgne's "Unbreakable" cipher

•Based on Baudot code for Teletypes

•Added (XORed) a random Key (sequence of bits) to a binary message

- Perfectly secure, provided:

•key is perfectly random

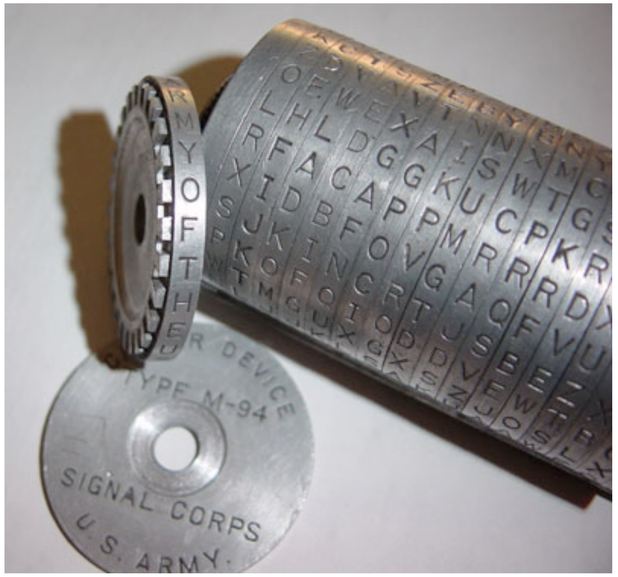
•key is at least as long as the message

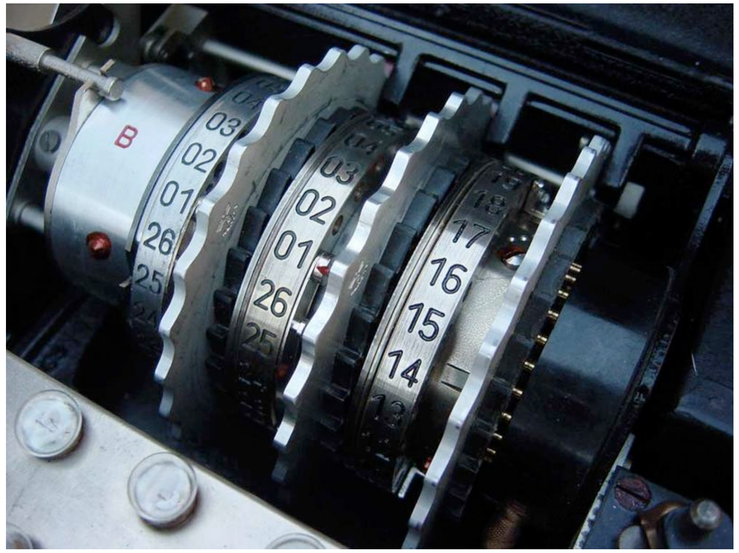
•key is never re-used

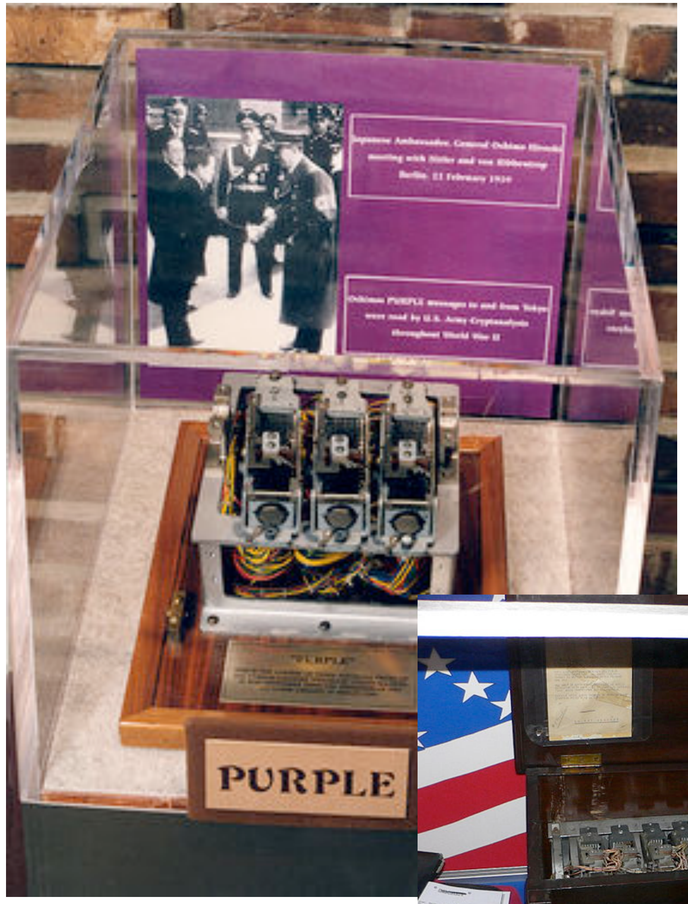
One-Time Ciphers

Mechanical Cryptography

- 1900s
  - Mass production and usage of cipher devices
  - Rotor ciphers
  - Electronic devices

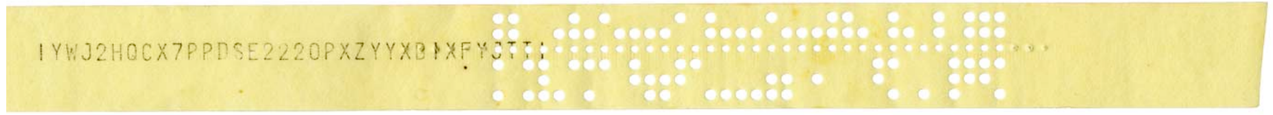






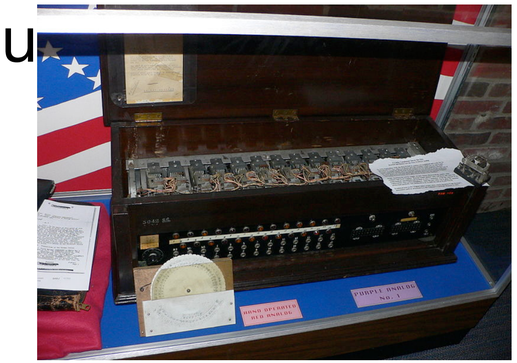
HAGELIN M-209 CIPHER MACHINE (GVG / PD)

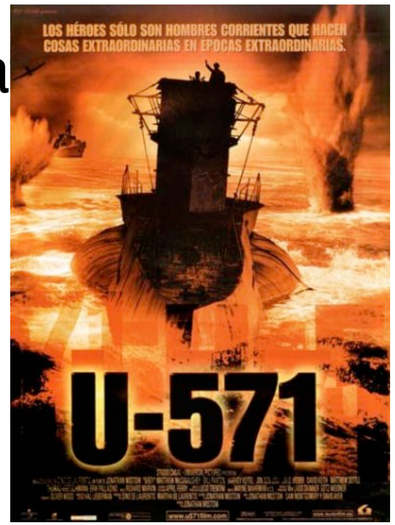

0015
AB CD EF GH I J KL MN OP QR ST UV WX YZ
AB CD EF GH I J KL MN OP QR ST UV WX YZ
0 AB
1 CD
2 EF
3 GH
4 I J
5 KL
6 MN
7 OP
8 ST
9 UV



Summary

- Most cryptosystems ultimately broken
  - Sophistication of the attackers outpaces that of the cryptosystem
  - Security relies on <u>secrecy of design</u>
  - Not evaluated for chosen plaintext, known plaintext a
  - Key generation/distribution procedu
  - It’s an arms race...



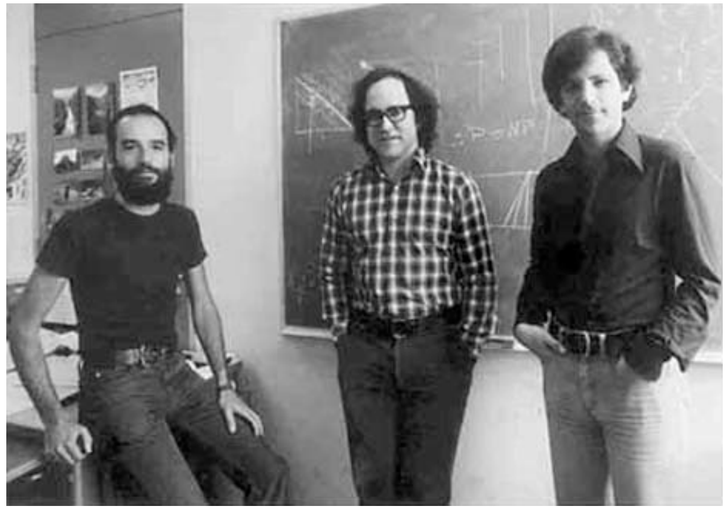


Kerckhoffs' Principle

2. It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;

"The enemy knows the System"
-- Claude Shannon's Maxim

The 1970s



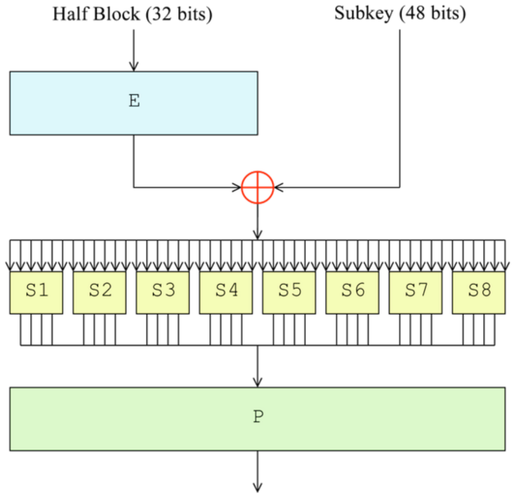
U.K. GCHQ

The Implications

- Exponential increase in study & usage of cryptography in industry, academia
- Wide-scale deployment of cryptographic systems
- Provable Security
  - Cryptographic Systems can be reduced to some hard mathematical problem

Data Encryption Standard

- Commercial-grade Block Cipher
  - 64-bit block size
  - 56 bit key (+ 8 bits parity)
  - “Feistel Network” Construction



Permutation

Permutation

Permutation Families

- Can’t have just one permutation
  - Alice & Bob know the permutation
    Adversary doesn’t
  - Permutation is “random” (ish)
  - But there are possible permutations
  - DES has a 56 bit key...

Block Cipher

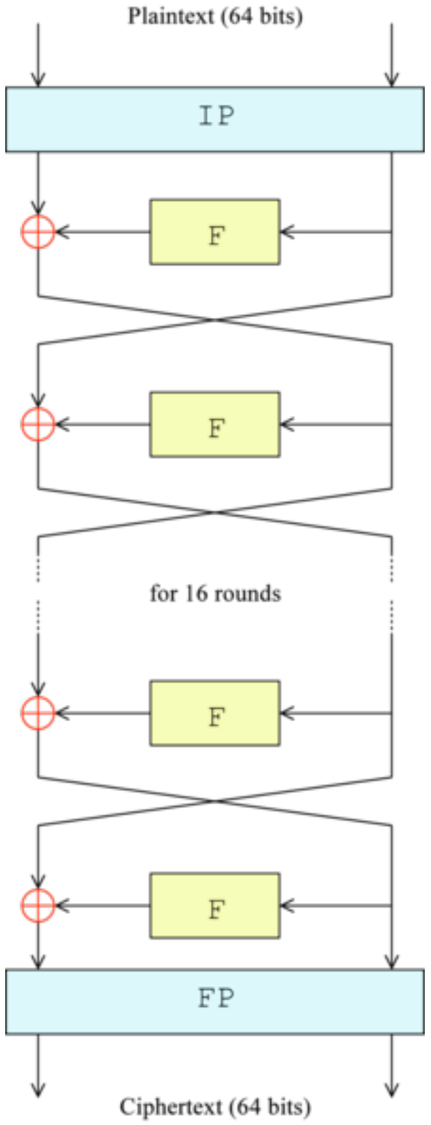
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - “Pseudo-random”

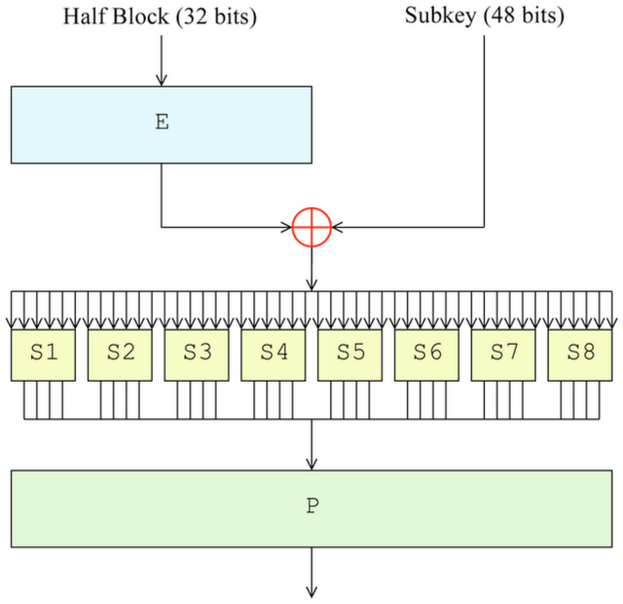
Block Cipher

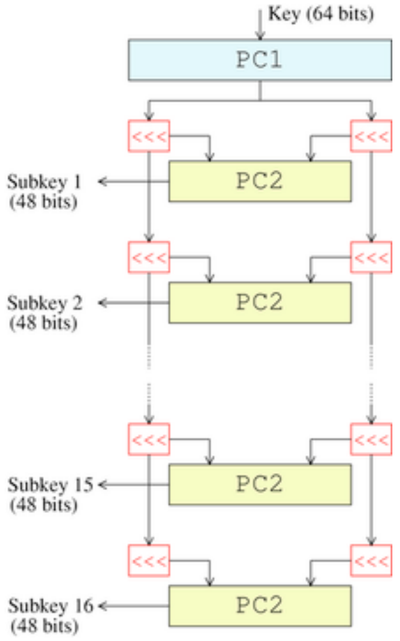
- Block cipher is a family of permutations
  - Indexed by a key (DES = 56 bit key)
  - Ideally: “Pseudo-random permutation (PRP)”

    (i.e., attacker who does not know the key can’t determine whether you’re using a random permutation, or a PRP)

DES: 64-bit Block, 56-bit Key

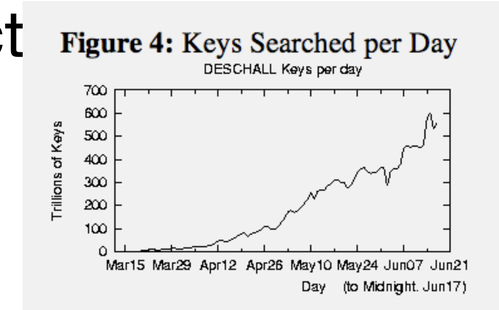


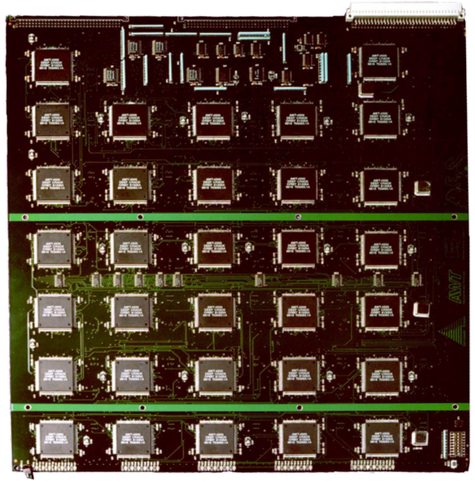




DES

- Some “clever” attacks on DES
  - However: practical weakness = 56 bit key size
  - Pract ES (now being deprecated)





U.S. Data-Scrambling Code Cracked With Homemade Equipment

By JOHN MARKOFF

SAN FRANCISCO -- In a 1990s variant of a John Henry-style competition between man and machine, researchers using a homemade supercomputer have cracked the government's standard data-scrambling code in record time -- and have done it by out-calculating a team that had harnessed thousands of computers, including some of the world's most powerful.