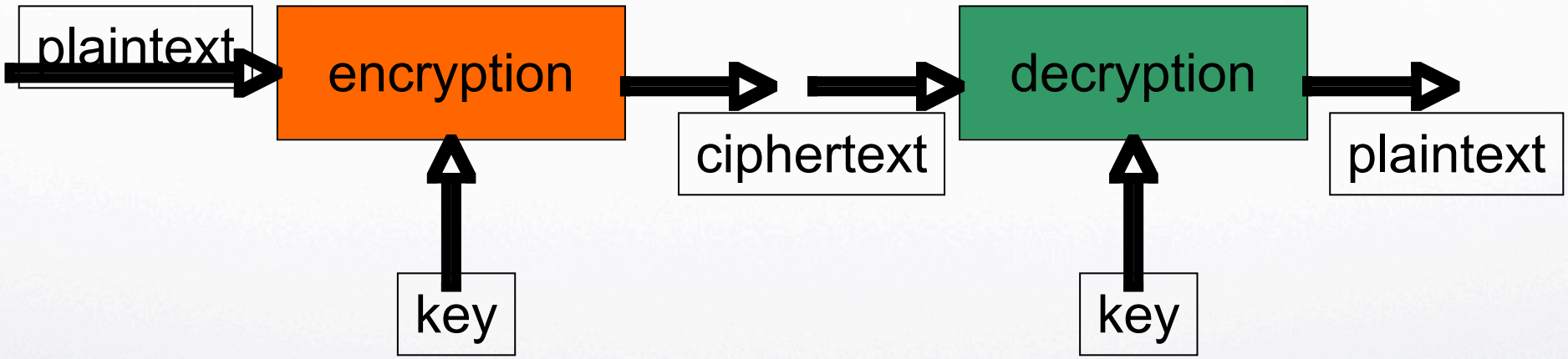
Computer Security

Symmetric Cryptography

Aggelos Kiayias

A symmetric Encryption Box



Properties

- Algorithms: $E_k(\cdot), D_k(\cdot)$
- Correctness: $D_k(E_k(M)) = M$
- Efficiency
  - asymptotic sense
    - e.g., "given a plaintext of n bits 2.35*n^2 steps are required."
- concrete
  - e.g., "this encryption box has an encryption rate of `100Kbits/s`"
- Intended Security "the ciphertext is a black-box"

How to Model Security

- Understand the adversary.
  - what are the resources?
  - what is the attack mode?
  - what is the goal of the attack?
- Kerckhoff's principle
  - A cryptosystem should be secure even if everything about the system except the key is known to the adversary.
  - Auguste Kerckhoffs, La cryptographie militaire, Journal des sciences militaires, vol. IX, pp. 5-38, Jan. 1883, pp. 161-191, Feb. 1883.

Key length

- The key-space is finite, e.g., $k \in \{0,1\}^n$
- Brute-force attack:
- Given $C = E_k(M)$
- Try for all $k \in \{0,1\}^n$

$$D_k(C) = ?$$

- Required time 2^n decryptions

Putting it to Perspective

- For AES software decryption can be done in 352 clock cycles for 128-bit.
- If key is 40bits then you need about 2 days in a 2Ghz Pentium.
- If key is 50bits then you need about half a year running 12 2Ghz Pentiums.
- If key is 128bits then you need about 2^71 years for 1000 2Gz Pentiums (about the size of the universe in miles)

Caesar Cipher

- ABCDEFGHIJKLMNOPQRSTUWXYZ
- DEFGHIJKLMNOPQRSTUWXYZABC

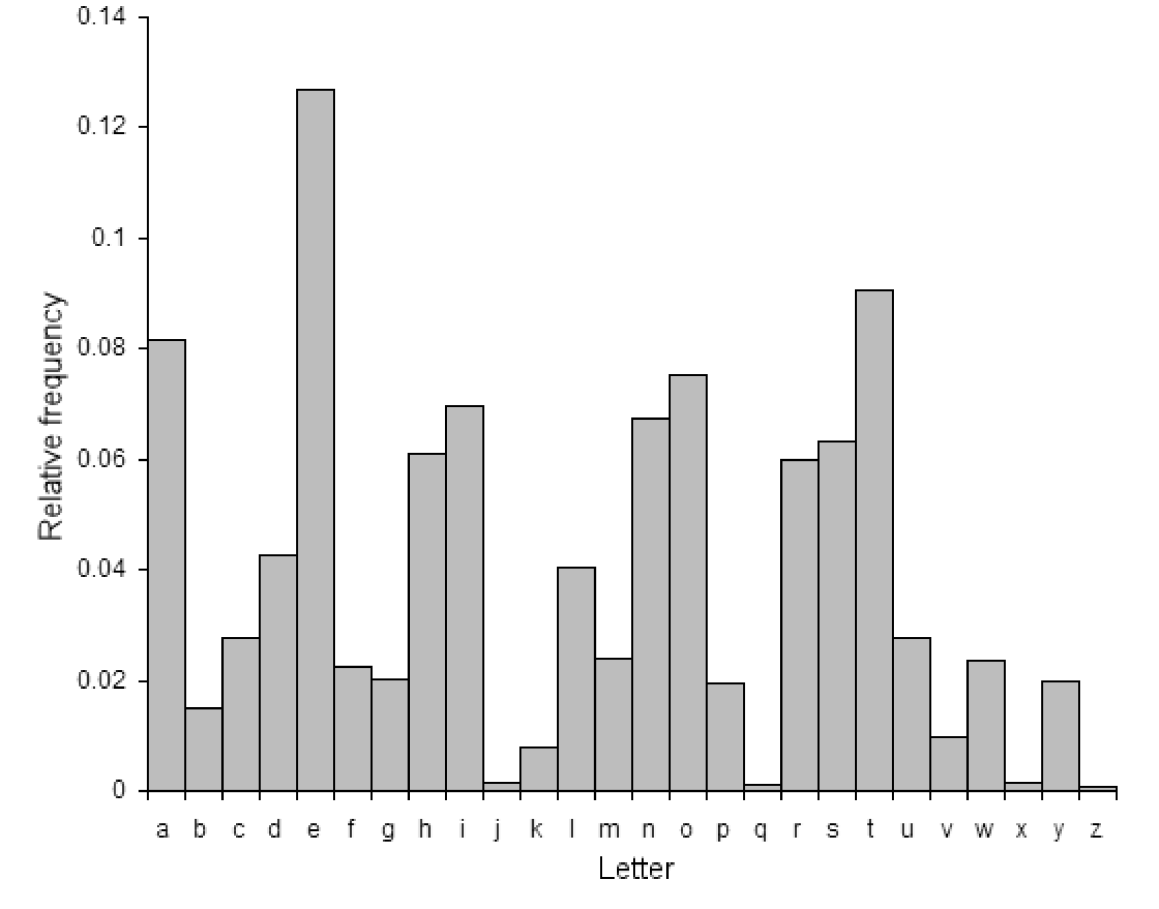
- TREATY IMPOSSIBLE =>
- WUHDWB LPSRVVLEOH

Monoalphabetic Cipher

Security of Monoalphabetic Ciphers

- Key space: $26! = 4.03 \cdot 10^{26}$
- This amounts to an 88 bit key.
- However such ciphers are totally insecure.

Frequency Analysis



One Time Pad

- G. Vernam 1917, AT&T.
- The only one true unbreakable cipher.

```
plaintext  01011101101111000101010101011011
key        10110101101011100010101010001011
ciphertext 11101000000100100111111111010000
```

Perfect security (for random key) proved by
C. Shannon (1949).
Shortcoming : for perfect security (key-size)=(plaintext-size)

Ciphers & Warfare

Retrospect -- WW11

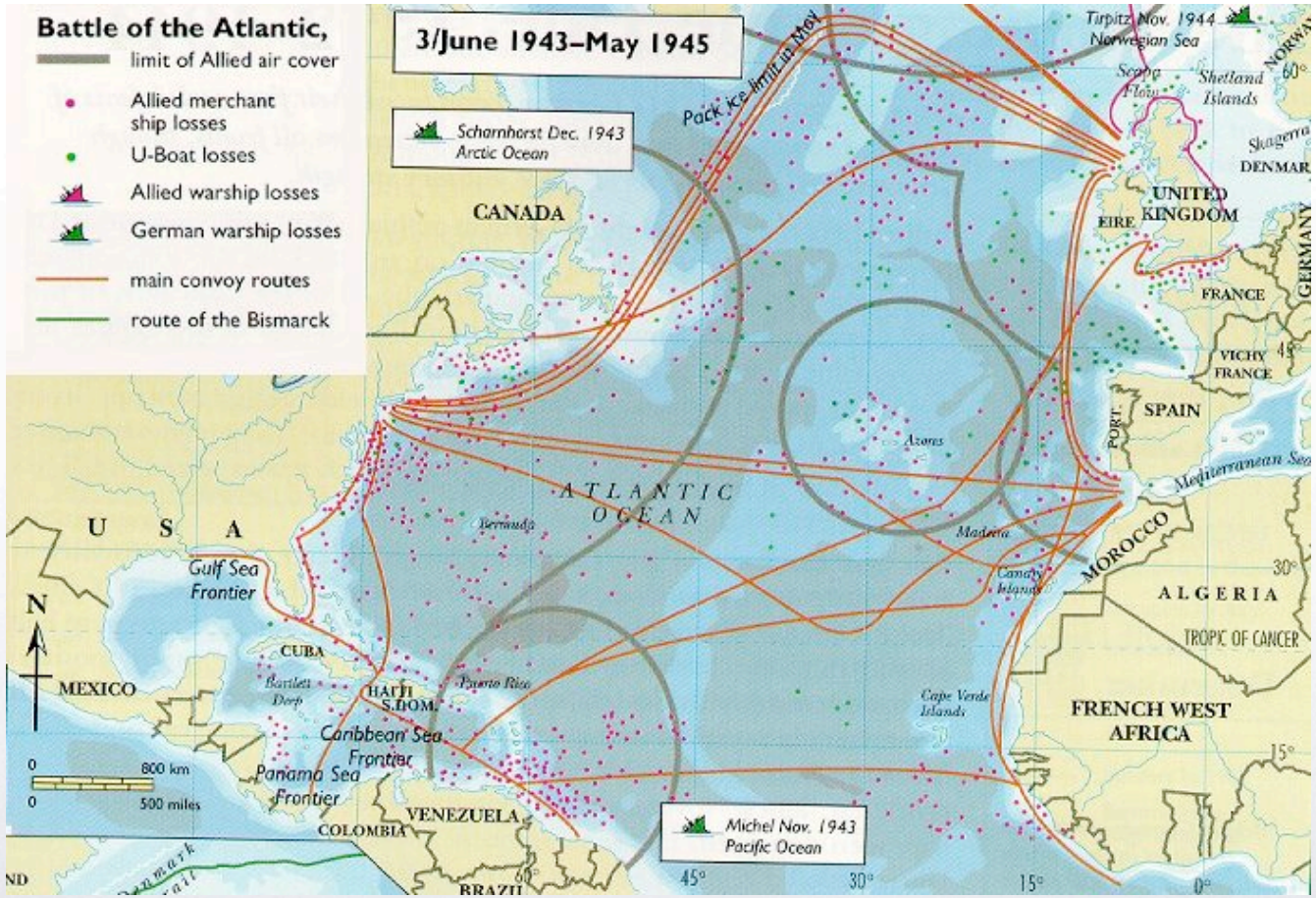
 ©2006-15 Aggelos Kiayias

Battle of the Atlantic

http://www.theworldatwar.com/images/

Maps showing the losses of Allied merchant ships in '39-'41

Battle of the Atlantic

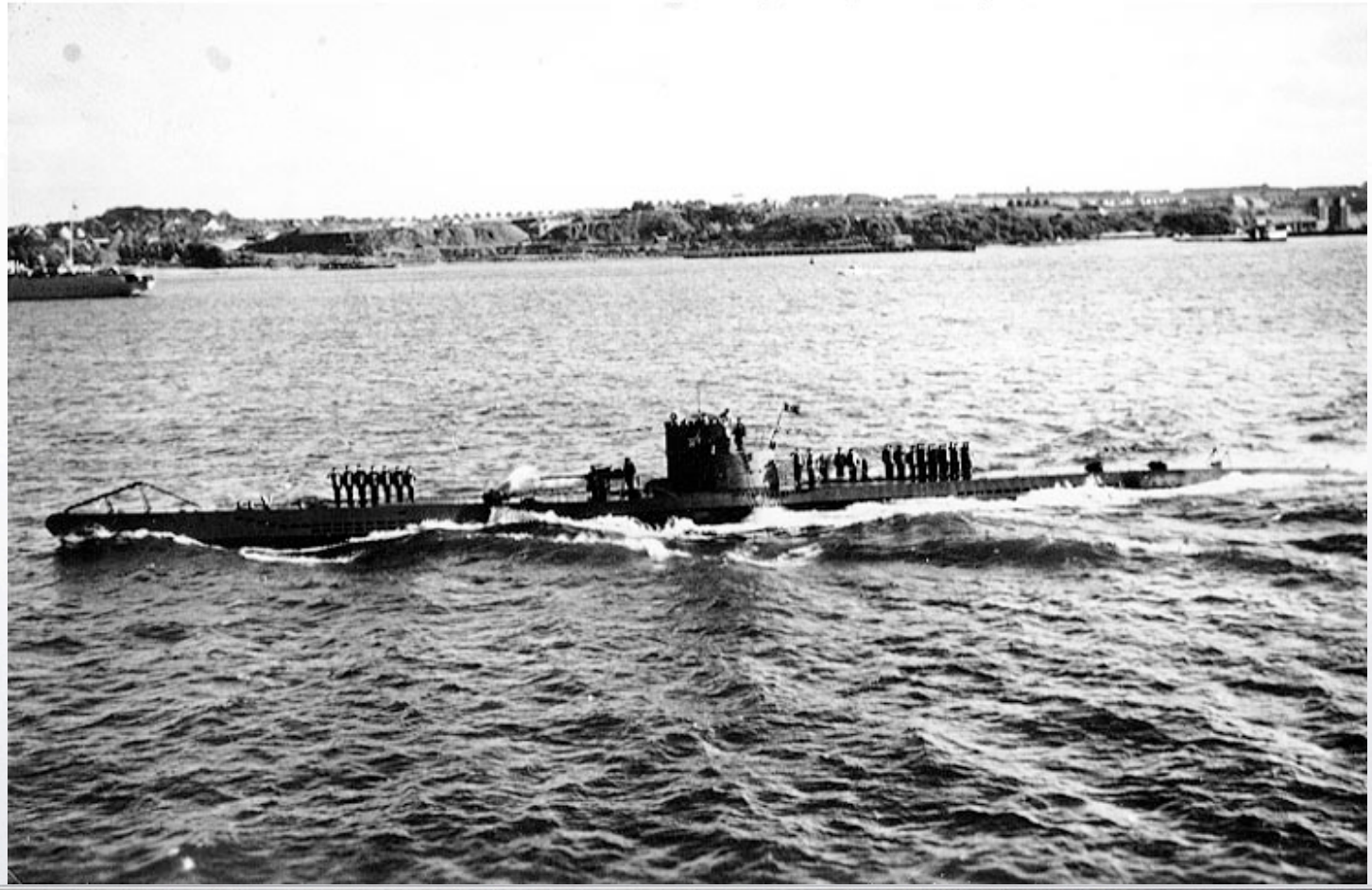


Submarine Warfare

Karl Doenitz

U-Boot
Wolfpack
strategy

Photo # NH 102539 German submarine (probably U-47) returns to port, 1939

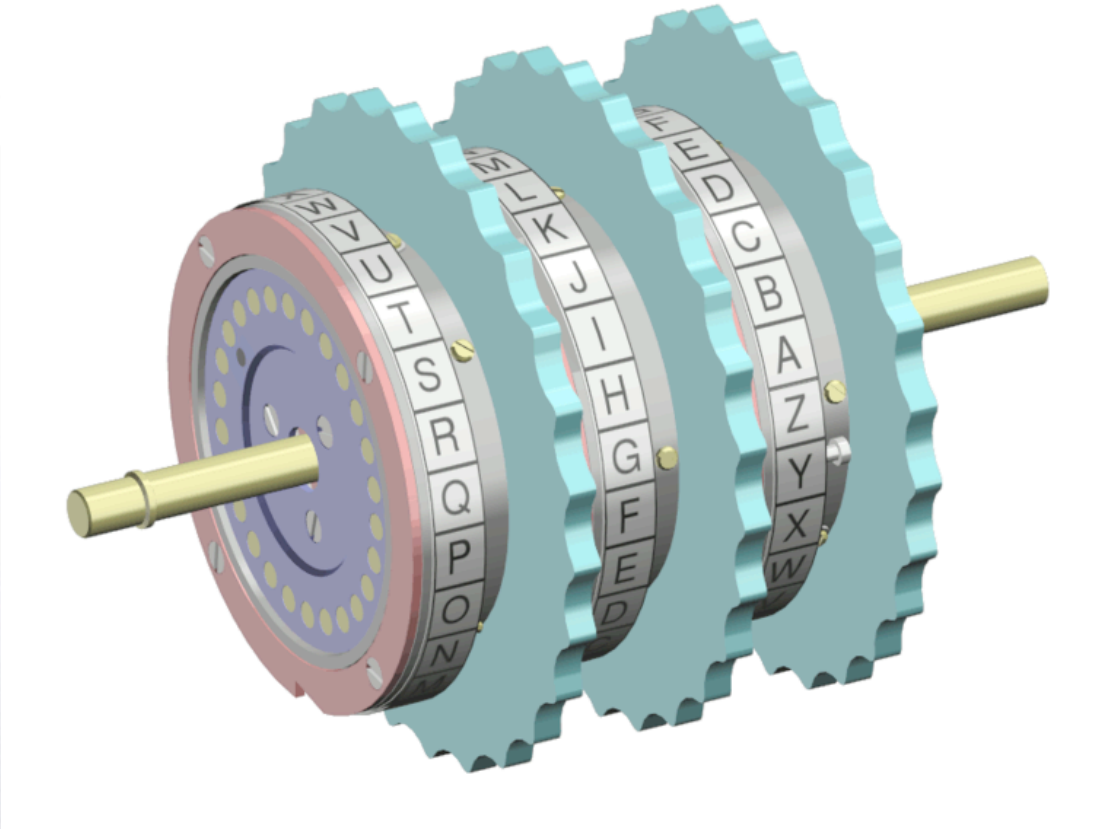


Importance for WW II

- W. Churchill
- *... the only thing that ever really frightened me during the war was the U-boot peril.*

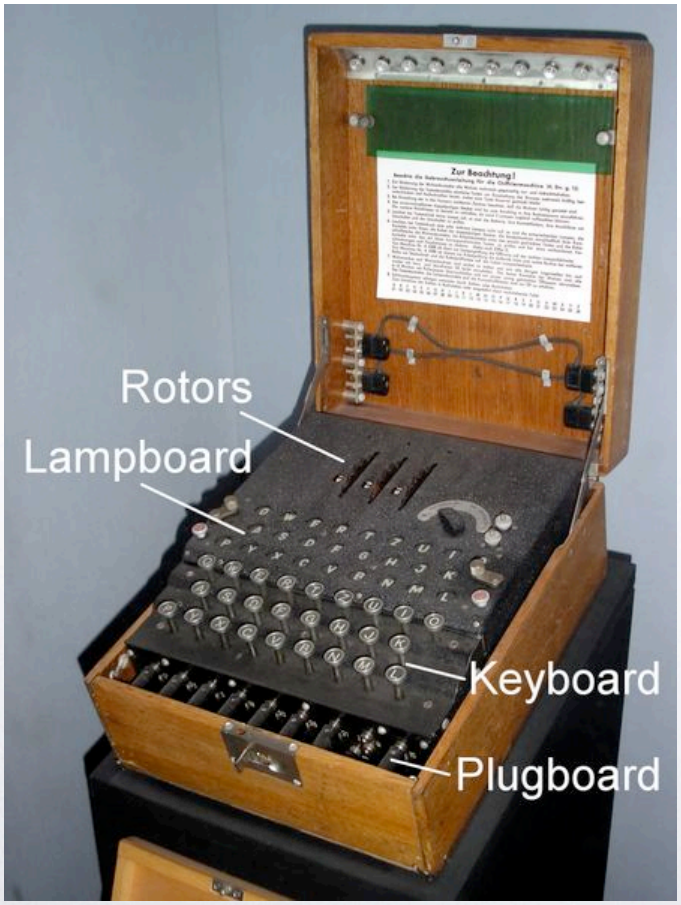
Rotor Encryption

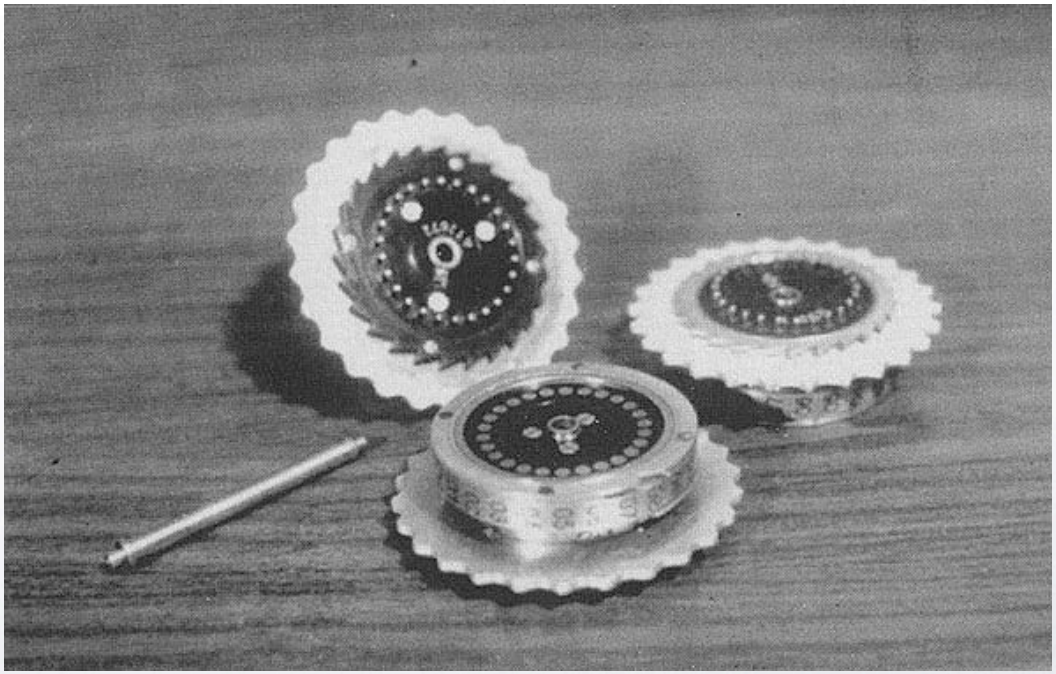
a
Polyalphabetic
cipher



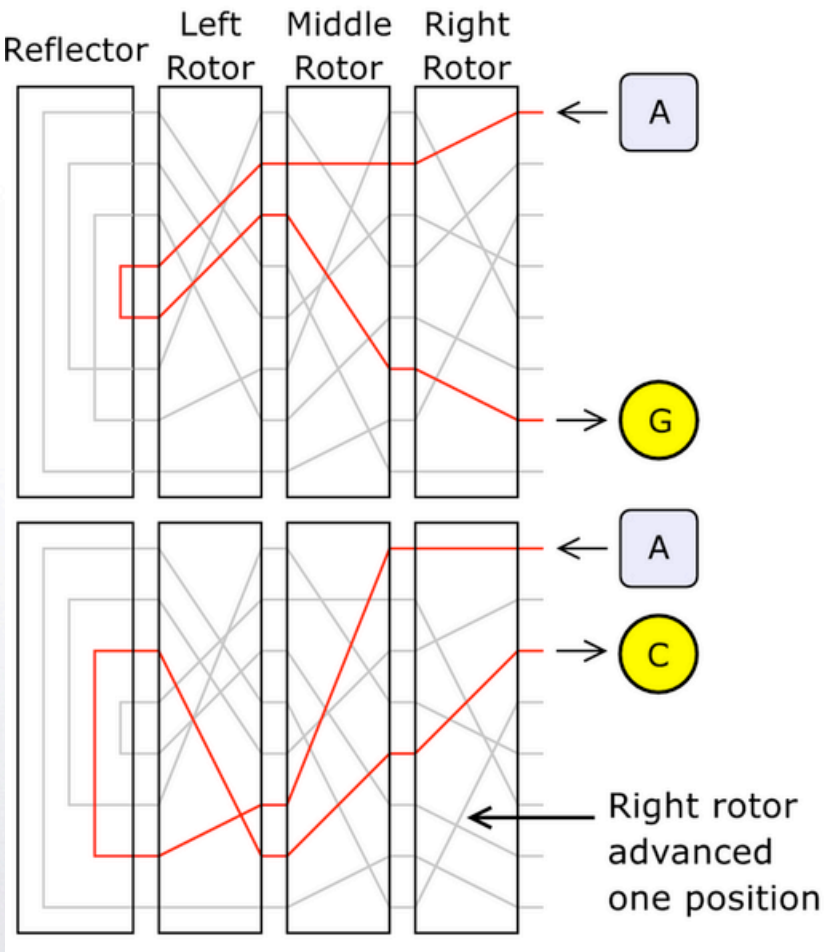
invented
independently
by many
~1915...

The Enigma Machine





Enigma Operation



The reflector enables the same configuration to be used for both decryption and encryption

Quiz : If an Rotor encrypted over alphabet A-Z ciphertext is XQRDA what do you know already about the plaintext?

Key Space

- Total number of possible Rotor machine configurations (English alphabet):
  - 26^{k} where k is the number of rotors. (assuming odometer *stepping*).
    - What is the key ?
    - How many keys are there?
- Other additions : plugboard (*steckerbrett*)

Permutations

Initial configuration (excl. plugboard) :

$$\pi_1 \cdot \pi_2 \cdot \pi_3 \cdot \sigma \cdot \pi_3^{-1} \cdot \pi_2^{-1} \cdot \pi_1^{-1}$$

After one stroke :

$$(\rho \cdot \pi_1 \cdot \rho^{-1}) \cdot \pi_2 \cdot \pi_3 \cdot \sigma \cdot \pi_3^{-1} \cdot \pi_2^{-1} \cdot (\rho \cdot \pi_1^{-1} \cdot \rho^{-1})$$

Where ρ is the (single) rotation permutation

...

recall $\rho^{26} = 1$

Cryptanalysis of Enigma

- (first step) reverse engineering (or recovery) of π_1, π_2, π_3
- (second step) Discovering the initial configuration (three exponents of ρ)

first reverse engineering successes :

Polish Cipher Bureau (Biuro Szyfrów)

http://www.impan.gov.pl/Great/Rejewski/article.html

During World War II :

Bletchley Park (over 10,000 people working during war)

Did Cryptanalysis win the war ?

- We will never know.
- Probably not.
  - But definitely shortened it (2 years?)
  - Saved million lives.
  - perhaps saved Berlin from an Atom Bomb.

Read: David Kahn's *Seizing the Enigma* - Watch: Imitation Game

Cipher Design Techniques I

- Substitution
- Break/encode message into a string from alphabet Σ
- Apply some permutation $\pi : \Sigma \rightarrow \Sigma$
- to each character of the message
- Total : $|\Sigma|!$ permutations to choose from

Vigenère cipher

- Key = a small sequence of rotations.
- Use the rotations successively.

KEYWORD LETTER	PLAINTEXT LETTER																									
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cipher Design Techniques, II

- Transposition
- Encode message into a string from alphabet Σ
- Suppose length is n
- Apply a permutation to the string

$$\pi : \{1, \ldots, n\} \rightarrow \{1, \ldots, n\}$$

Spartan Scytale

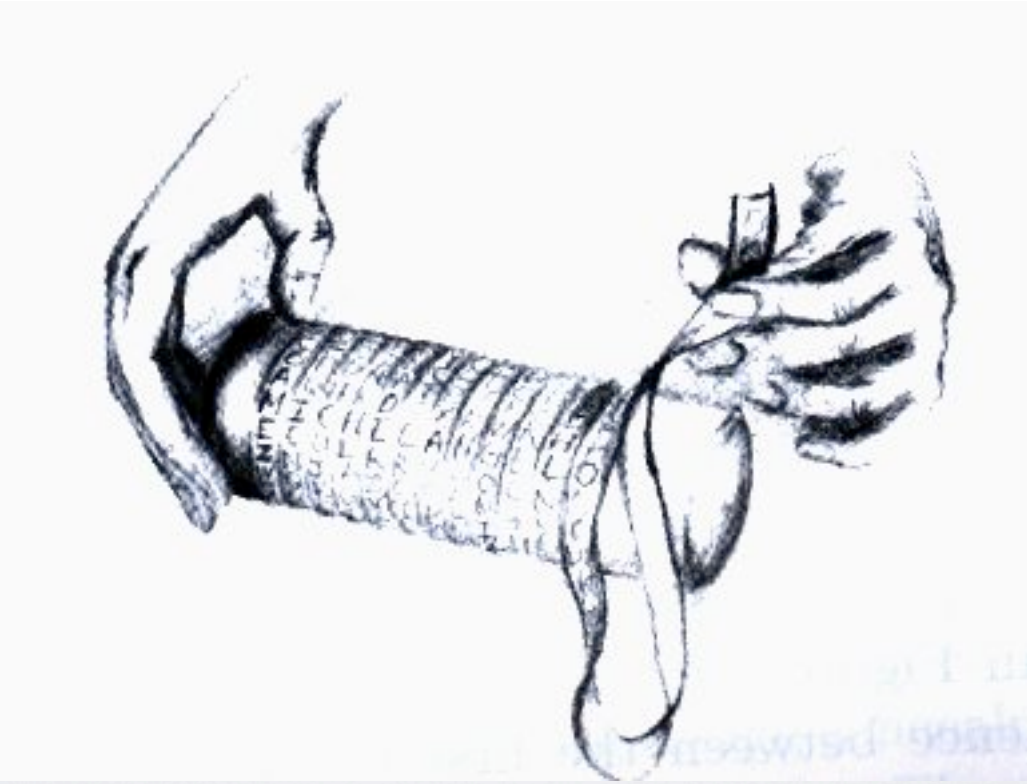


image from http://courses.gdeyoung.com

Composition

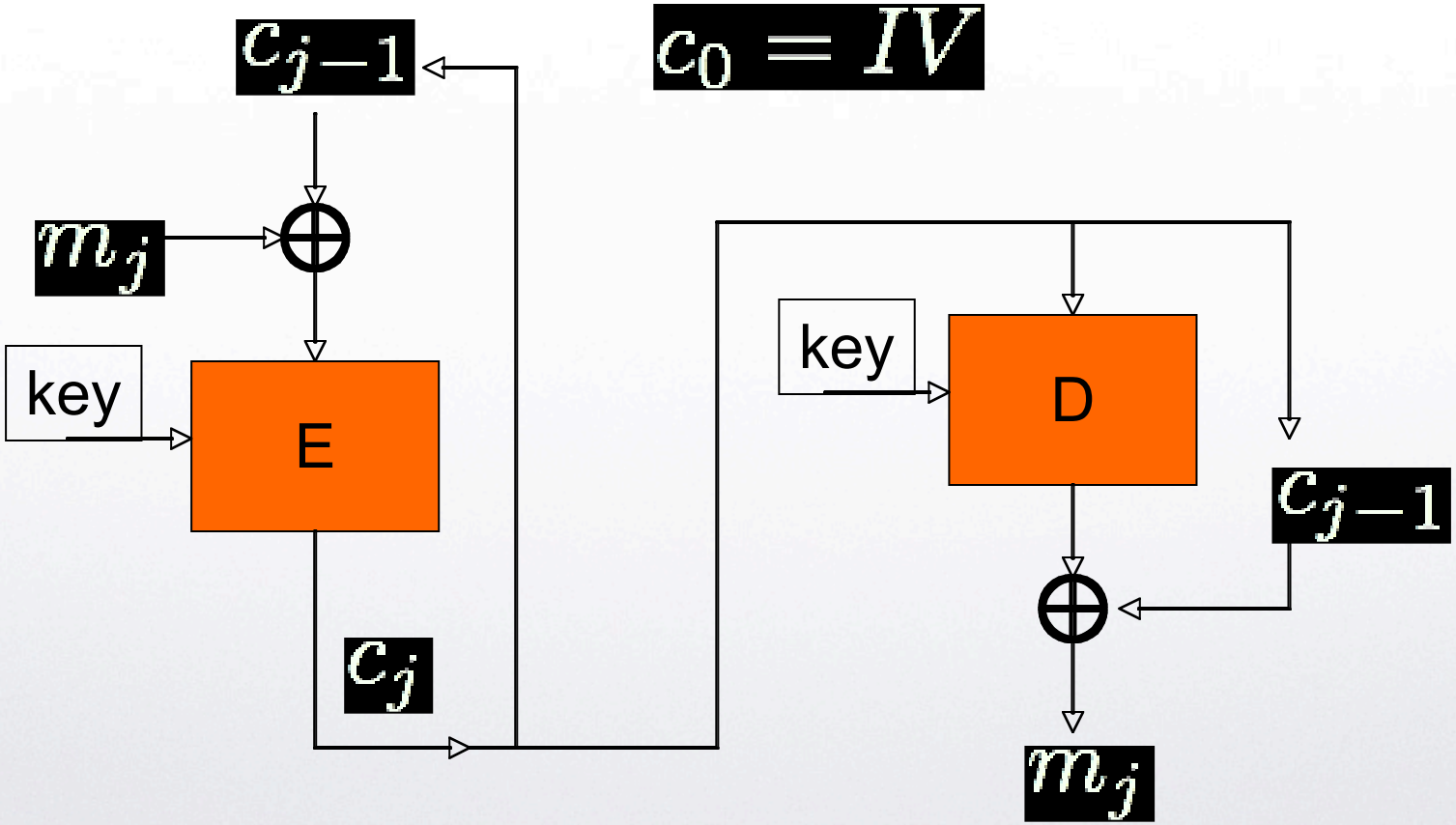
- One can build a cipher using various
  - encodings & decodings to various alphabets coupled with series of
    - substitutions
    - transpositions
- What makes a good cipher?
  - resistance to known attacks.
  - adherence to general principles e.g., diffusion: spreading information from single plaintext character to all ciphertext.

Block Ciphers

- operate on a single block of a fixed number of bits. (e.g., AES operates on a 128-bit input block).
- require the specification of a mode of operation to encrypt longer messages.
  - electronic codebook mode
  - cipher block chaining
  - counter mode
  - …

Example Mode of Operation

Ciphertext Block Chaining



Choosing the IV

- Using a random IV for each CBC execution has the advantage of providing a "randomized encryption"
- Two identical messages are encrypted differently.
- The additional communication overhead is tiny (one block)

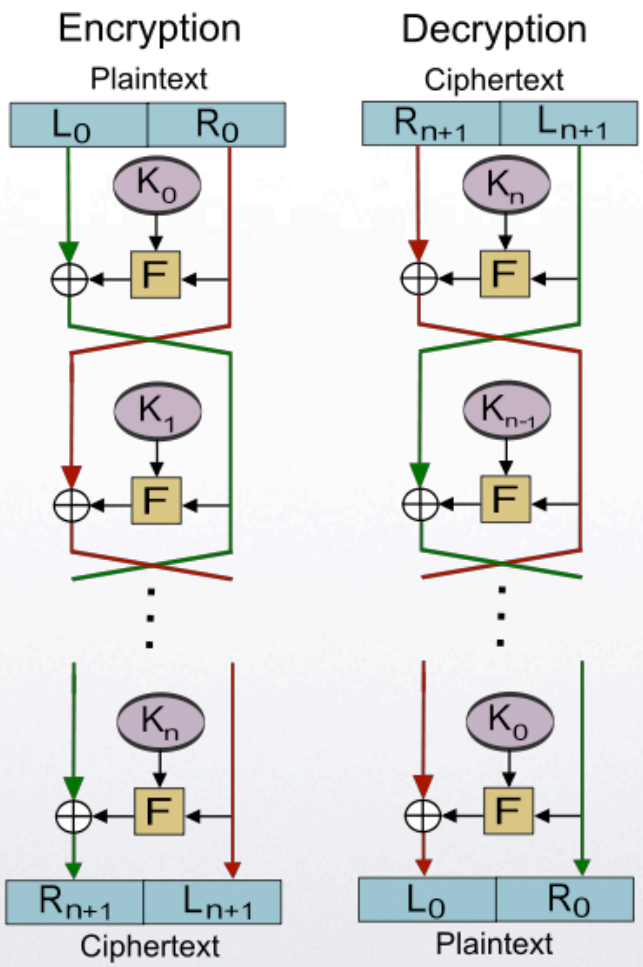
Data Encryption Standard (DES)

- Adopted in 1977.
- Design by IBM.
  - Key-length is 56-bits.
  - block size is 64-bits.
  - The design found to be exceptionally good.
    - The key-size was criticized always that was too short (even in '77 it was believed to be breakable with $20 million equipment).

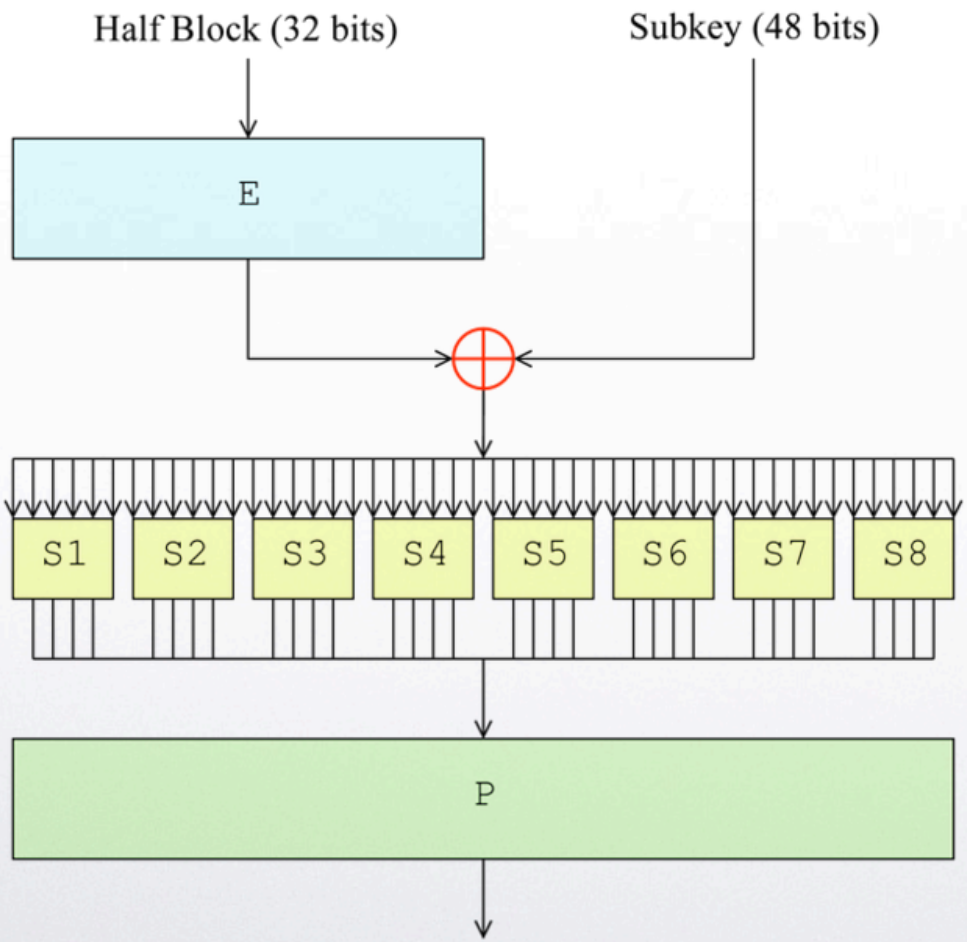
Feistel Ciphers

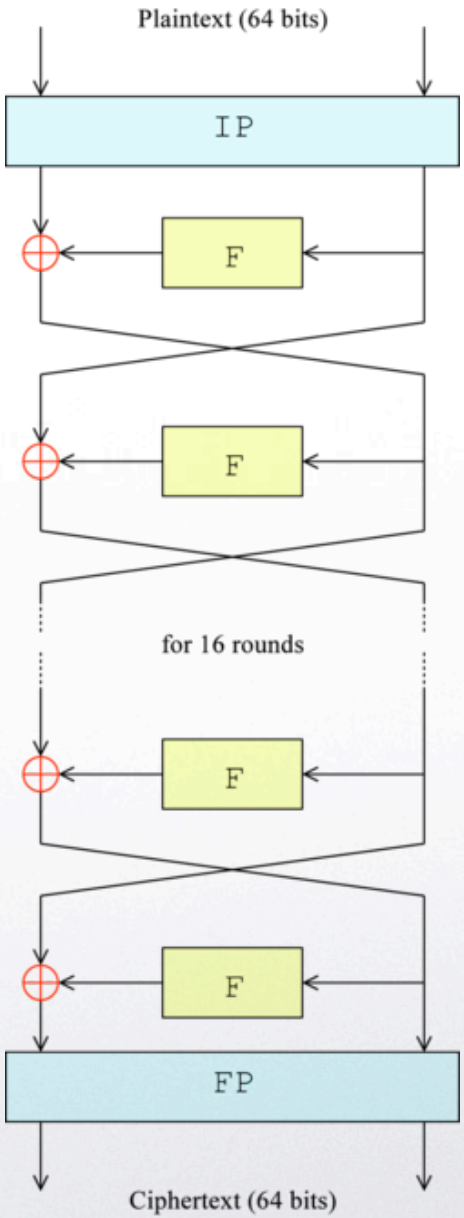
Encryption/Decryption can be achieved by the same circuit

F : does not need to be invertible.



DES


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


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

Brute-Force against DES

- 1997: in four months time, 3500 machines in distributed fashion infer a DES-key (DESCHALL project).
  - the cheap - distributed approach.
- 1998: The DES Cracker breaks a key in 56 hours. Cost $100,000.
- 1999: distributed.net (DES Cracker + distributed help) : 22 hours.

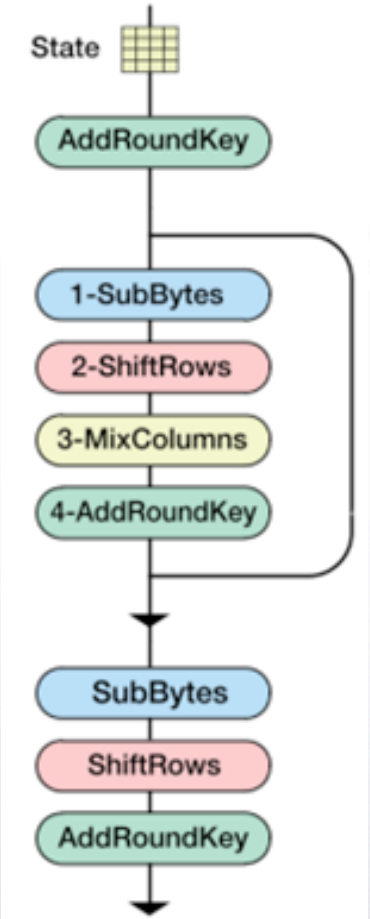
More advanced attacks

- Linear Cryptanalysis (Matsui '93)
  - DES : Given 2^{43} Known plaintext-cihphertext pairs. Choice of plaintext = random.
  - 2^{43} operations in 12 99Mhz CPUs
    - 50 days for the recovery of the key in 1994 (M. Matsui, Crypto '94).
- Differential Cryptanalysis (Biham-Shamir '90)
  - DES: ~ cracked with 2^{47} chosen plaintexts.
    - Techniques typically not applicable in many practical settings
    - But: extremely important as indicators of cipher strength.

Advanced Encryption Standard

- Block cipher (128-bit)
- Key-sizes (128, 192, 256 bits).
- Adopted in December 2001
- Two year International competition for the standard.
- Many competitors (including IBM, RSA Labs)
- Winner was the Rijndael algorithm from two Belgian cryptographers.

AES Design (High Level)



- Encode input as 16 byte string.
- Perform the following steps 10 times:
- (SubBytes) A fixed substitution step. $[2^8] \longrightarrow [2^8]$
    - The Rijndael S-Box
- (ShiftRows) A fixed transposition step. $[2^4] \longrightarrow [2^4]$
- (MixColumns) Consider input as four 4-byte sequences. Fixed substitution based on a linear transformation $[2^{10}] \longrightarrow [2^{10}]$
- (AddRoundKey) X-Or with the key (bit operation)
- Each round uses a different round-key (that is derived in a standard way from the key)

Stream Ciphers

- Typically faster than block ciphers.
  - Lower diffusion than block ciphers.
- The "one-time pad" design approach:
  - or binary-additive stream ciphers
  - Key is treated as a seed to a pseudorandom generator.
  - A pseudorandom bit sequence of sufficient length is generated.
  - Message is X-Ored with the string.

 ©2006-15 Aggelos Kiayias

Linear Feedback Shift Registers

- Length of register.
- Number/Locations of X-Or gates

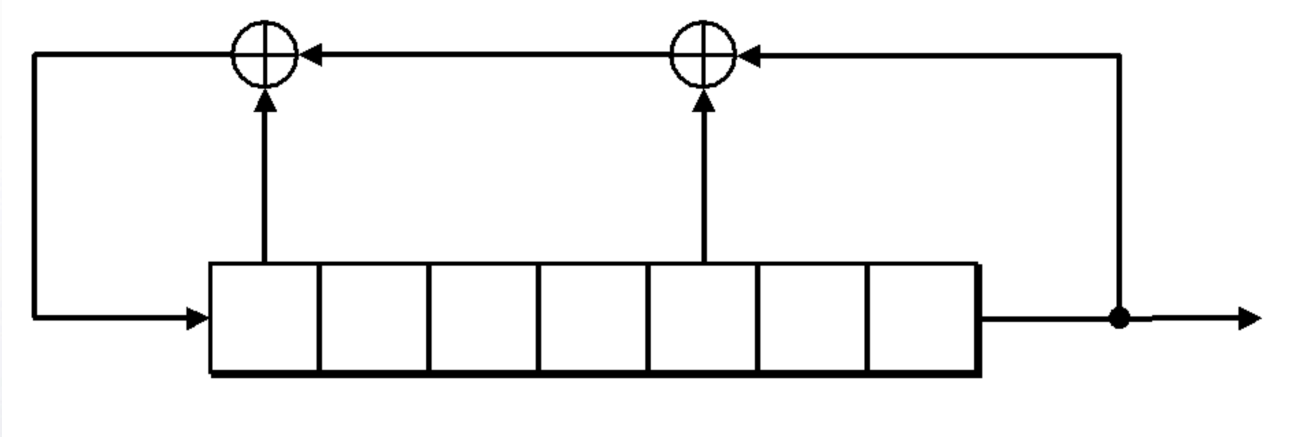


image from http://www.rsasecurity.com/rsalabs/faq/images/lfsr.gif

Periodic Behavior

- All LFSRs repeat after a certain number of clock ticks.
- For a proper selection of X-Or locations the maximum period length can be reached for any non-zero seed:
  - period length = 2^{L} - 1 for L-long register.

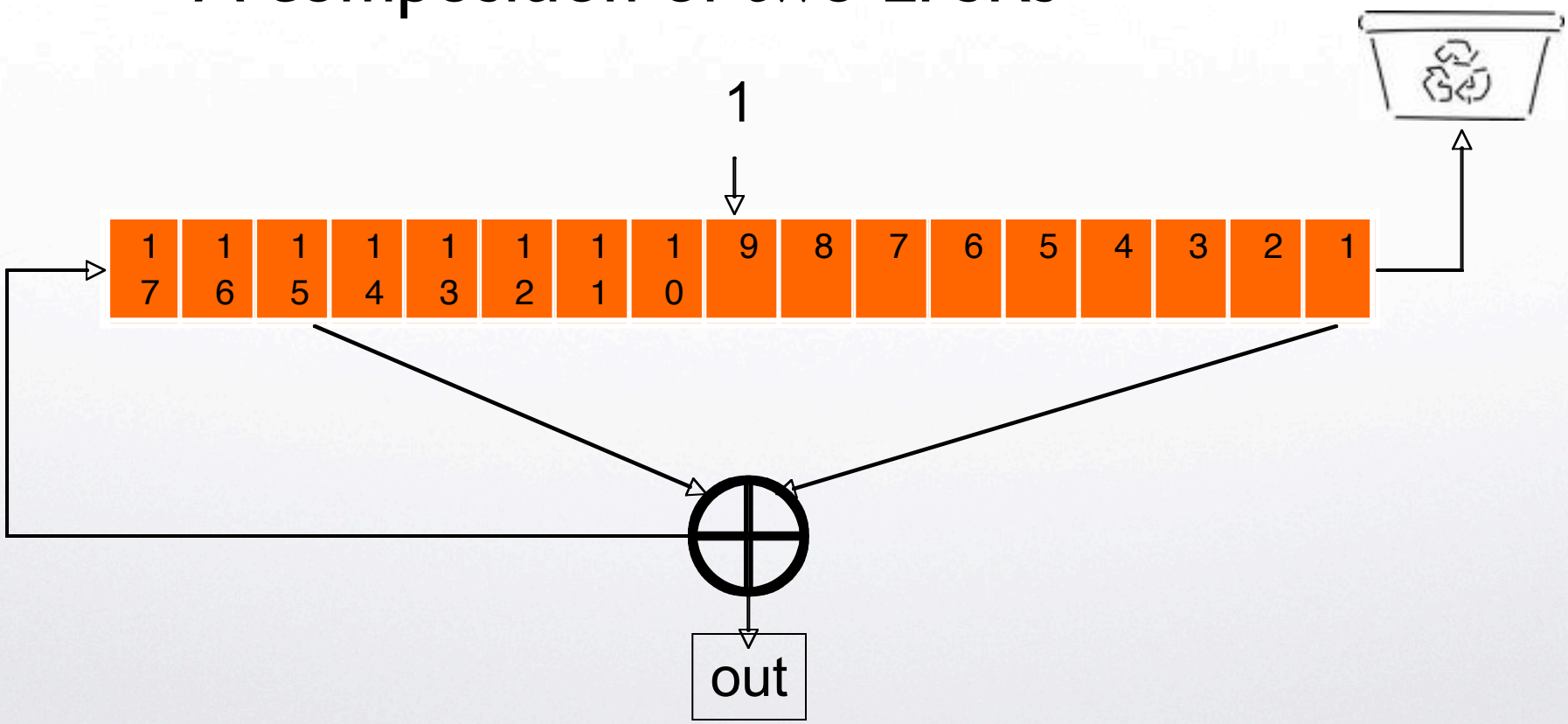
LFSR for stream ciphers

- Using a single LFSR as a basis for a stream cipher is not appropriate:
  - The locations X-Ors can be determined using a 2*L subsequence of the LFSR output.
  - Thus, any known plaintext-ciphertext substring will yield the internals of the LFSR
  - The remainder of the sequence can now be generated.

 ©2006-15 Aggelos Kiayias

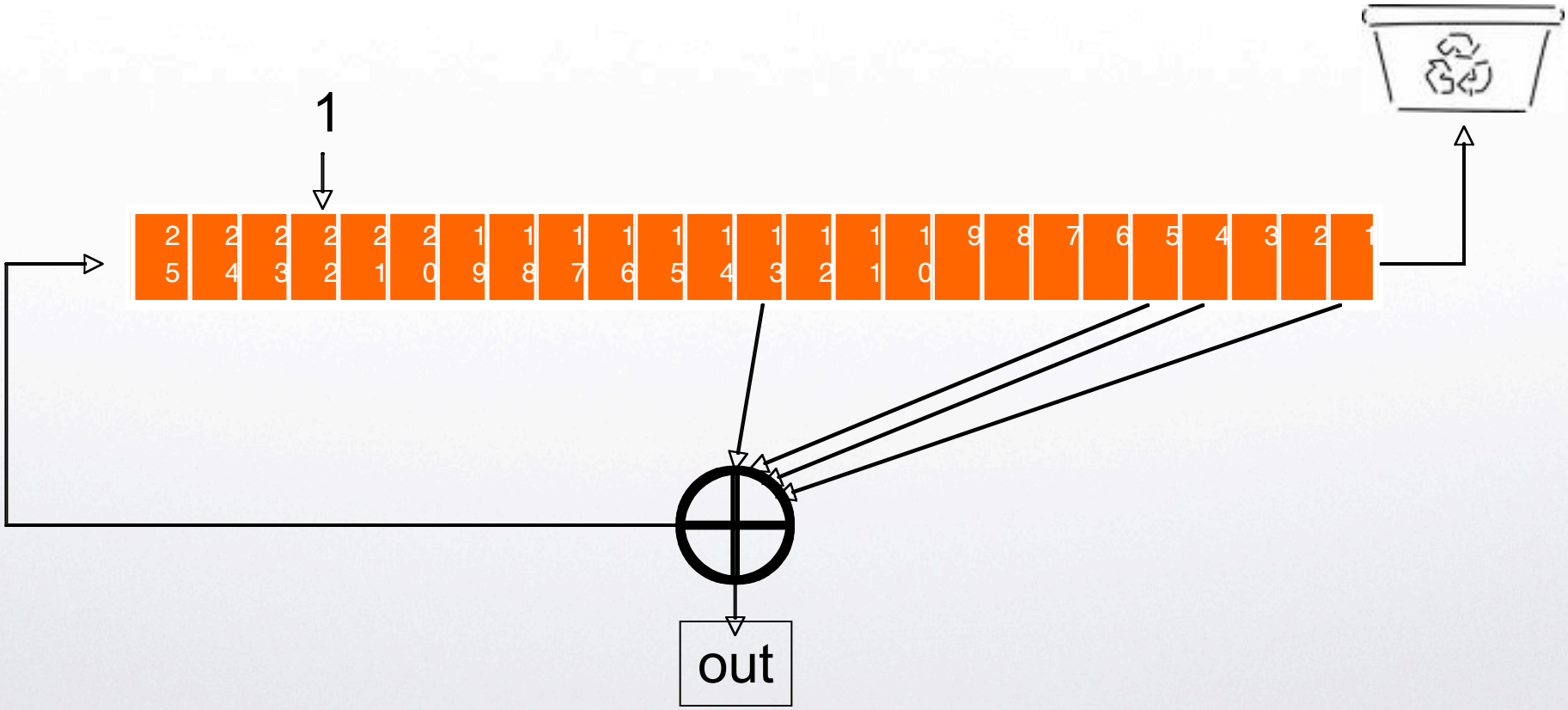
CSS Content Scramble System

- A composition of two LFSRs



CSS, II

Key-Size = 40 bits = 25+17-2



Composing the two LFSR

- 8 clock ticks will produce 2 bytes from the two LFSRs.
- c + B1 + B2 = 9 bits =
- [8 bits key stream] , next_c

CSS Decryption

- Typical stream line fashion with an additional fixed substitution step.
- Each DVD is encrypted with a random 40-bit key (that seeds the two LFSRs)
- How this key is derived?

CSS Key distribution

- There is a hidden block with 409 ciphertexts that contain `<Kdisk,hash>`.
- Each ciphertext is encrypted with one of 409 `Kplayer` keys.
- Your DVD Player has one of the `Kplayer` keys.
- Once `Kdisk` is recovered it can be used to recover `Ktitle` or other keys that may encrypt different parts of a DVD.

Storyline

- October 99, J.L. Johansen, from Norway releases DeCSS.
- this lead to 4 year ordeal with the law - finally acquitted in 2004.
- DeCSS was outlawed.

DeCSS Implementations

http://www.cs.cmu.edu/~dst/DeCSS/Gallery/hannum-efdtt-source.txt

```
/*    efdtt.c    Author:  Charles M. Hannum <root@ihack.net>          */
/*                                                                     */
/*    Thanks to Phil Carmody <fatphil@asdf.org> for additional tweaks.   */
/*                                                                     */
/*    Length:  434 bytes (excluding unnecessary newlines)              */
/*                                                                     */
/*    Usage is:  cat title-key scrambled.vob | efdtt >clear.vob        */

**************************CENSORED DUE TO DMCA ***********************************
unsigned char x[5],y,s[2048];main(n){for(read(0,x,5);read(0,s,n=2048);write(1,s
**************************CENSORED DUE TO DMCA ***********************************
**************************CENSORED DUE TO DMCA ***********************************
**************************CENSORED DUE TO DMCA ***********************************
**************************CENSORED DUE TO DMCA ***********************************
*6^c+~y;}}
```

An illegal Prime Number

```
4856507896573978293098418946942861377074420873513579240196520736
6869851340104723744696879743992611751097377770102744752804905883
1384037549709987909653955227011712157025974666993240226834596619
6060348517424977358468518855674570257125474999648219418465571008
4119086259716947970799152004866709975923596061320725973797993618
8606316914473588300245336972781813914797955513399949394882899846
9178361001825978901031601961835034344895687053845208538045842415
6548248893338047475871128339598968522325446084089711197712769412
0795862440547161321005006459820176961771809478113622002723448272
2493232595472346880029277764979061481298404283457201463489685471
6908235473783566197218622496943162271666393905543024156473292485
5248991225739466548627140482117138124388217717602984125524464744
5055834628144883356319027253195904392838737640739168912579240550
1562088978716337599910788708490815909754801928576845198859630532
3823490558092032999603234471140776019847163531161713078576084862
2363702835701049612595681846785965333100770179916146744725492728
3348691600064758591746278121269007351830924153010630289329566584
3662000800476778967984382090797619859493646309380586336721469695
9750279687712057249966669805614533820741203159337703099491527469
1835659376210222006812679827344576093802030447912277498091795593
8387121000588766689258448700470772552497060444652127130404321182
6101035911864766629638584950874484973734768614208805294 43
```

The 09F9... case

- Another famous illegal number :

09F911029D74E35BD84156C5635688C0

The AACS (advanced access content system)
is the encryption used in Blu-Ray disks

much more sophisticated compared to DVDs
09F9... key was leaked in 2007.
currently key is revoked (would only play pre April 07 disks)

http://www.youtube.com/watch?v=L9HaNbsIfp0

Still keys are continuously leaked & patched

(what is known as pirate evolution) ...

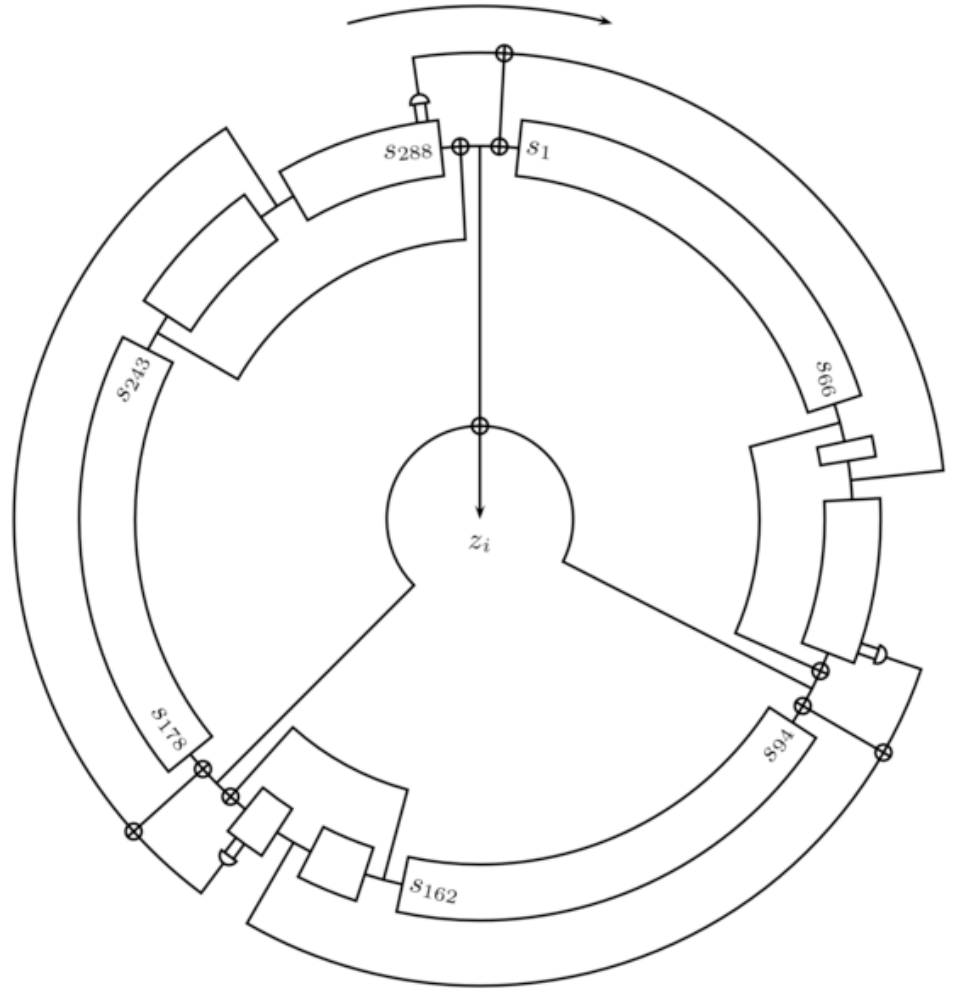
cf. Slysoft's AnyDVD

Composing LFSR & CSS

- 2 LFSRs have been used in various composition modes to produce strong stream ciphers.
- The CSS composition is not a secure one.
- Attacks that succeed with much less than 2^40 operations are possible using very little plaintext knowledge.
- Even if a better composition was used the key is too short (40-bits).

Shrinking Generator

- A strong 2 LFSR composition system.
- Two LFSRs `L,L'`.
- At each clock tick:
- if `L'=1` then output `L` else discard `L`

- Design requirement : `gcd(L,L')=1`
  - FACT: Any LFSR that simulates the shrinking generator requires ~ `2^{L'}` register size.

Trivium