BLOCK CIPHERS

MODERN BLOCK CIPHERS

- NOW LOOK AT MODERN BLOCK CIPHERS
- ONE OF THE MOST WIDELY USED TYPES OF
- CRYPTOGRAPHIC ALGORITHMS
- PROVIDE SECRECY /AUTHENTICATION SERVICES
- FOCUS ON DES (DATA ENCRYPTION STANDARD)
- TO ILLUSTRATE BLOCK CIPHER DESIGN PRINCIPLES

BLOCK CIPHER PRINCIPLES

- MOST SYMMETRIC BLOCK CIPHERS ARE BASED ON A **FEISTEL**
- **CIPHER STRUCTURE**
- NEEDED SINCE MUST BE ABLE TO **DECRYPT** CIPHERTEXT TO
- RECOVER MESSAGES EFFICIENTLY
- BLOCK CIPHERS LOOK LIKE AN EXTREMELY LARGE
- SUBSTITUTION
- WOULD NEED TABLE OF 264 ENTRIES FOR A 64-BIT BLOCK
- INSTEAD CREATE FROM SMALLER BUILDING BLOCKS
- USING IDEA OF A PRODUCT CIPHER

IDEAL BLOCK CIPHER

DATA ENCRYPTION STANDARD (DES)

- MOST WIDELY USED BLOCK CIPHER IN WORLD
- ADOPTED IN 1977 BY NBS (NOW NIST)
- AS FIPS PUB 46
- ENCRYPTS 64-BIT DATA USING 56-BIT KEY
- HAS WIDESPREAD USE
- HAS BEEN CONSIDERABLE CONTROVERSY OVER ITS
- SECURITY

DES HISTORY

- IBM DEVELOPED LUCIFER CIPHER
- BY TEAM LED BY FEISTEL IN LATE 60'S
- USED 64-BIT DATA BLOCKS WITH 128-BIT KEY
- THEN REDEVELOPED AS A COMMERCIAL CIPHER WITH
- INPUT FROM NSA AND OTHERS
- IN 1973 NBS ISSUED REQUEST FOR PROPOSALS FOR A
- NATIONAL CIPHER STANDARD
- IBM SUBMITTED THEIR REVISED LUCIFER WHICH WAS
- EVENTUALLY ACCEPTED AS THE DES

DES DESIGN CONTROVERSY

- ALTHOUGH DES STANDARD IS PUBLIC
- WAS CONSIDERABLE CONTROVERSY OVER DESIGN
- IN CHOICE OF 56-BIT KEY (VS LUCIFER 128-BIT)
- AND BECAUSE DESIGN CRITERIA WERE CLASSIFIED
- SUBSEQUENT EVENTS AND PUBLIC ANALYSIS SHOW IN
- FACT DESIGN WAS APPROPRIATE
- USE OF DES HAS FLOURISHED
- ESPECIALLY IN FINANCIAL APPLICATIONS
- STILL STANDARDISED FOR LEGACY APPLICATION USE

DES ENCRYPTION OVERVIEW

INITIAL PERMUTATION IP

- FIRST STEP OF THE DATA COMPUTATION
- IP REORDERS THE INPUT DATA BITS
- EVEN BITS TO LH HALF, ODD BITS TO RH HALF
- QUITE REGULAR IN STRUCTURE (EASY IN H/W)
- EXAMPLE:
- IP(675A6967 5E5A6B5A) = (FFB2194D 004DF6FB)

DES ROUND STRUCTURE

- USES TWO 32-BIT L & R HALVES
- AS FOR ANY FEISTEL CIPHER CAN DESCRIBE AS:
- $L_i = R_{i-1}$
- $R_i = L_i \oplus F(R_i, K_i)$
- R_{i-1}, F TAKES 32-BIT R HALF AND 48-BIT SUBKEY:
- EXPANDS R TO 48-BITS USING PERM E
- ADDS TO SUBKEY USING XOR
- PASSES THROUGH 8 S-BOXES TO GET 32-BIT RESULT
- FINALLY PERMUTES USING 32-BIT PERM P

DES ROUND STRUCTURE

SUBSTITUTION BOXES S

- HAVE EIGHT S-BOXES WHICH MAP 6 TO 4 BITS
- EACH S-BOX IS ACTUALLY 4 LITTLE 4 BIT BOXES
- OUTER BITS 1 & 6 (**ROW** BITS) SELECT ONE ROW OF 4
- INNER BITS 2-5 (**COL** BITS) ARE SUBSTITUTED
- RESULT IS 8 LOTS OF 4 BITS, OR 32 BITS
- ROW SELECTION DEPENDS ON BOTH DATA & KEY
- FEATURE KNOWN AS AUTOCLAVING (AUTOKEYING)
- EXAMPLE:
- S(18 09 12 3D 11 17 38 39) = 5FD25E03

DES KEY SCHEDULE

- FORMS SUBKEYS USED IN EACH ROUND
- INITIAL PERMUTATION OF THE KEY (PC1) WHICH SELECTS
- 56-BITS IN TWO 28-BIT HALVES
- 16 STAGES CONSISTING OF:
- ROTATING **EACH HALF** SEPARATELY EITHER 1 OR 2 PLACES
- DEPENDING ON THE **KEY ROTATION SCHEDULE** K
- SELECTING 24-BITS FROM EACH HALF & PERMUTING THEM BY
- PC2 FOR USE IN ROUND FUNCTION F
- NOTE PRACTICAL USE ISSUES IN H/W VS S/W

DES DECRYPTION

- DECRYPT MUST UNWIND STEPS OF DATA COMPUTATION
- WITH FEISTEL DESIGN, DO ENCRYPTION STEPS AGAIN USING
- SUBKEYS IN REVERSE ORDER (SK16 … SK1)
- IP UNDOES FINAL FP STEP OF ENCRYPTION
- 1ST ROUND WITH SK16 UNDOES 16TH ENCRYPT ROUND
- …
- 16TH ROUND WITH SK1 UNDOES 1ST ENCRYPT ROUND
- THEN FINAL FP UNDOES INITIAL ENCRYPTION IP
- THUS RECOVERING ORIGINAL DATA VALUE

DES EXAMPLE

AVALANCHE IN DES

AVALANCHE EFFECT

- KEY DESIRABLE PROPERTY OF ENCRYPTION ALG
- WHERE A CHANGE OF **ONE** INPUT OR KEY BIT RESULTS
- IN CHANGING APPROX **HALF** OUTPUT BITS
- MAKING ATTEMPTS TO "HOME-IN" BY GUESSING
- KEYS IMPOSSIBLE
- DES EXHIBITS STRONG AVALANCHE

STRENGTH OF DES – KEY SIZE

- 56-BIT KEYS HAVE 256 = 7.2 X 1016 VALUES
- BRUTE FORCE SEARCH LOOKS HARD
- RECENT ADVANCES HAVE SHOWN IS POSSIBLE
- IN 1997 ON INTERNET IN A FEW MONTHS
- IN 1998 ON DEDICATED H/W (EFF) IN A FEW DAYS
- IN 1999 ABOVE COMBINED IN 22HRS!
- STILL MUST BE ABLE TO RECOGNIZE PLAINTEXT
- MUST NOW CONSIDER ALTERNATIVES TO DES

STRENGTH OF DES – ANALYTIC ATTACKS

- NOW HAVE SEVERAL ANALYTIC ATTACKS ON DES
- THESE UTILISE SOME DEEP STRUCTURE OF THE CIPHER
- BY GATHERING INFORMATION ABOUT ENCRYPTIONS
- CAN EVENTUALLY RECOVER SOME/ALL OF THE SUB-KEY BITS
- IF NECESSARY THEN EXHAUSTIVELY SEARCH FOR THE REST
- GENERALLY THESE ARE STATISTICAL ATTACKS
- DIFFERENTIAL CRYPTANALYSIS
- LINEAR CRYPTANALYSIS
- RELATED KEY ATTACKS

STRENGTH OF DES – TIMING ATTACKS

- ATTACKS ACTUAL IMPLEMENTATION OF CIPHER
- USE KNOWLEDGE OF CONSEQUENCES OF
- IMPLEMENTATION TO DERIVE INFORMATION ABOUT
- SOME/ALL SUBKEY BITS
- SPECIFICALLY USE FACT THAT CALCULATIONS CAN TAKE
- VARYING TIMES DEPENDING ON THE VALUE OF THE
- INPUTS TO IT
- PARTICULARLY PROBLEMATIC ON SMARTCARDS

SUMMARY