- Block
- Message Authentication Code
- DES
CBF - Cerebral blood flow

EGC - Electrocardiogram

Can be used in different modes

More applicable block supplies
None

expression (e.g. lower function)

Proof of existence of
First Project
- Can be decapitated
- First permutation
- 16 Pounds (use 16 subjects)
- Just permutation

First Project

Des
E Boxes (expansion perm)
P Boxes (permutation)
S Boxes (substitution)
A diagram representing a cryptographic algorithm, showing connections between Key, Compression, S-Box, P-Box, Expansion, and output 32 bits. There are notes on the right-hand side, mentioning 40 bits, 8 key bits, and an input process.
Week

2001 Peace -> 1.5 cm

Eff -> Caracas - 1998 - 45 cm

des

25% water even 26% areverse

How are possible keys

DES -> break vs brute force
(1) All ciphers can be brute force

except one

one time pad
I LOVE YOU [parity]

HATE YOU [good parity]
OTP use is not feasible

key too big

by storage security transmission
Key: \( \{ K_1, K_2, K_3 \} \)

\[ \text{Cipher text} = 116.625 \]

\[ \text{Key size} = 56 + 3 = 168 \text{ bits} \]

\[ \text{DES - tripleDES} \]
128 - 256 - 512 - 1024

AES much faster

3DES, slow
AES accepted in 2001 after 8 years of testing by Joan Daemen, Vincent Rijmen, and Rijndael cipher.
Children can be "closed"