Random bit = binary bit of \(x_1, x_2, x_3, \ldots\)
Choose plaintext (4 cipherparts) → Known ciphertext (or cipher only)

Copy transformations

Choose key

Plaintext

P, C

2 0 1 1 1 0 0 0 0 0 0 0 0
Linear Cryptanalysis

Do not

- Linear Pearson Product + Linear Approximation

Linear Cryptanalysis

\[ \text{Lin} \]
- make little changes in present
- change placement
- adapt your choice comprehensively
1. \( \text{each} \rightarrow \text{company} \rightarrow \text{no advocate} \)

2. \( \text{comp} \rightarrow \text{everyone} \rightarrow \text{visible} \)

3. \( \text{everyone} + \text{company} + \text{step} \)

4. Considerations
State $\rightarrow$ exit

Exit $\rightarrow$ state

Explora 2012
Chapter Chimp - Headquarters

Loop a broadcaster

(Experimental)

Algo evacuation area
Cannot be password.

- always see not reversible
- cryptic bloody
- etc.

(technically bloody) for understanding

\[ \text{Hash Function} \]
n ≥ 100

1 and 2. Random input will influence the forecast.

In the forecast, each
2. different branch exists.
Success is when you stand up after you fall.

Adapted from: Find any book...

Input: Hash of given number

? \rightarrow 0
module 2^32 + denotes addition.


cash operation.

rotation by 8 places: s

denotes a left bit

each operation.
cash constant, different for

K / denoted a 32-bit

M / denotes a 32-bit block

each round.
one function is used in

F is a nonlinear function.

(32 bits)
16 operations. A, B, etc.
grouped in four rounds of
these operations,
MD5 consists of 64 of

1286
One iteration within the SHA-1 compression function. A, B, C, D, and E are 32-bit words of the state. \( n \) varies for each operation. \( W_t \) is the expanded message word of round \( t \). 

- \( K_t \) denotes a left bit rotation by \( n \) places.
- \( \text{denotes addition modulo 2}^{32} \).

SHA-256

SHA-512

160-bit output

Secure Hashing Algorithm
Bit strength of hash functions

Because of birthday attacks.

Md-5 \rightarrow 128-bit
160-bit > 80 bits
64 bits
23 people → 50% chance of collision

2.365

of people of collision of by chance in a group

Birthday Paradox