Chosen
\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

Standard
\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

Lots of \[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]

\[ SHA-3 \leftarrow SHA-2 \leftarrow SHA-256 \]

\[ SHA-3 \rightarrow SHA-2 \rightarrow SHA-256 \]
$K_t$ is a constant.

Shift

$\gg\gg$ denotes left circular shift.

$E$ is a nonlinear function.

Pair of words of the state:

$A$, $B$, $C$, $D$, and $E$ are 32-bit variables within the SHA-1 compression function.
Birthday attacks

- Hash collisions are hard to find
- Hash collision finding is a great attack
  - Use Birthday attack
Birthday Attack
Problem

We have a source document.

Doc hash: h(D)

Find another Doc that has the same hash as D.
Alice argues to sign the box. Bed went Alice to sign the box.
Bob征求了1版的建议后，做了修改。
Birthday collision in NÎHWG

Birthday \text{ force } = 2^{\text{ n bits }} \text{ current file}

\begin{align*}
\text{Birthday} & = \frac{2^n}{\text{ current file}} \\
& = \frac{1.2 \text{ n}}{10}
\end{align*}
Everyone, here is a clarification:

If 64-bit encryption is good,
In public (yes, even in restaurant)

Can we communicate properly?

Any empathy
\[ \text{Heilige Puzzles} \]

\[ \Rightarrow \text{nummer, schilden = nummer} \]

\[ \Rightarrow \text{easy to verify} \]

\[ \Rightarrow \text{easy to solve} \]

\[ \Rightarrow \text{easy to build} \]

\[ \Rightarrow \text{pure & more} \]

\[ \Rightarrow \text{pure & more} \]
L. Seeds to Alice

Cameras E Sn (hidden)

Finds Sn + puzzle 4 seasons + 1306 picks one season
Alice finds m
then Alice + Bob use
\((8\|m)\) as key
[Works for ..... ]
The force is given by

\[ F_{net} = \overline{F} (t) \]
good

and

signs

# of faces

= \frac{1}{2} n - 2

n

time for basic force

exchange energy

metallophosphates
Alice = Alice (vertical) median
Bob = Bob (horizontal) median

if median key

Alice chooses

pick the number in front

else: known key exchange