Birthday attacks

Hyoungshick Kim
Department of Software
College of Software
Sungkyunkwan University

Birthday attacks

- This is the best "generic" collision attack on a hash function $H: \{0,1\}^* \rightarrow \{0,1\}^n$?
- Compute $H(x_1), \ldots, H(X_{2^\wedge(n/2)})$
  - What is the probability of a collision?
- Related to the so-called *birthday paradox*
  - How many people are needed to have a 50% chance that some two people share a birthday?

"Birthday attacks" analysis (1)

- How many possibilities that are all different?
  - $(K)_N$ = K(K-1)…(K-N+1): the number of all possible samples without replacement when we choose N different samples
- Probability of no repetition?

$$\frac{k*(k-1)*(k-2)*\cdots(k-n+1)}{k*k*k\ldots*k}=$$

$$\frac{k}{k}*\frac{k-1}{k}*\cdots*\frac{k-n+1}{k}=1*\left(1-\frac{1}{k}\right)*\left(1-\frac{2}{k}\right)*\cdots*\left(1-\frac{n-1}{k}\right)\leq$$

$$\boxed{1-\frac{a}{k}\leq e^{-\frac{a}{k}}}$$

$$e^{-\frac{1}{k}}*e^{-\frac{2}{k}}*e^{-\frac{3}{k}}*\cdots*e^{-\frac{n-1}{k}}\cong e^{-\frac{n^2}{2k}}$$

“Birthday attacks” analysis (2)

$$e^{-\frac{n^2}{2k}} \leq \frac{1}{2} \iff \frac{n^2}{2k} \geq \ln 2 \iff$$

$$n^2 \geq 2\,(\ln 2)k = 1.38k \iff$$

$$n \geq \sqrt{1.38k}$$

- Bottom line: For <u>k=365, n=23</u> suffices
- In general $\underline{n = \boldsymbol{\Omega}(\sqrt{k})}$ suffices

Theorem for birthday attacks

- Thm. When the number of balls (in balls and N bins) is $O(N^{1/2})$, the probability of a collision is 50%. (see the CLR book)
- Need 2n-bit output length to get security against attackers running in 2^n time
  - Twice the length of block cipher keys
  - A block cipher with 128-bit key provides equivalent security to a hash function with 256-bit output.

Questions?


Sungkyunkwan
Campus
established
Sciences
University
university
campus
School
Suwon
Seoul
Natural
Korean
Graduate
English
Social
Global
Building
Institute
constructed
edit
Professors
Confucian
Humanities
lecturers
Engineering
Education
located
Joseon
Business
Science
schools
Administration
Academic
ASLE-Korea
Advanced
Language
also
two
four
city
now
one
Zone
trees
Samsung
Anniversary
University's
establishment
abides
symbol
Japanese
Korea
College
storeys
capital
Complex
campuses
Hall
Course
Literature
original
levels
heart
expansion
Humanity
Undergraduate
Technology
became