Applied cryptanalysis

—

or

—

how to win an iPhone

The challenge

- July 14, Engineyard posts: “Programming Contest! Win iPhone 3GS & $2,000 Cloud Credit”
- Contest to start on July 20 and runs for 30 hours.
- Task: find phrase s.t. SHA-1(phrase) is close to SHA-1(target phrase) in Hamming distance.
- Our friend Paul wants the iPhone; our cluster (10 Core2 Quads) had had some issues and needed some testing.
- July 19, Dan finds some time to write fast SHA-1 code.
- Results need to be submitted through Twitter; getting accounts.
- 6 hours before the challenge starts: Paul doesn’t want the Cloud Credit, we may ask Bo-Yin and Doug for help. Time for Dan to learn CUDA . . .

More details

- SHA-1 operates on blocks of 64 bytes at a time.
- Output of hashing first block used as initialization vector (IV) for second block etc.
- ASCII characters are stored in 8 bits (=1 byte), i.e.

  `BUGS`

  takes 4 bytes.
- Phrase in challenge must have 12 words from Engineyard's dictionary; words separated by blanks.
- 5 free characters may be appended.
- Free to change casing of letters in the dictionary words, i.e. can use

  `BUGS, BUGs, BUgS, BUgs, BuGS, ...`
- Can repeat dictionary words in phrase.

Strategies

- 2nd preimage attacks on SHA-1 are not practical.
- Can only succeed by guessing. Do as many tests per second as possible.
- Reuse first block as often as possible, i.e. fix first 64 bytes, vary the end. (No chance of exhausting in 30h).
- Make the 12 words and 12 blanks fit exactly in first block; the second one consist entirely of the 5 characters.
- 64 bytes in 12 words: choose 8 words of length 4 and 5 of length 5.
- Start each process with random choice of upper and lowercase letters among these.
- Would have been screwed with only very short or very long words.

Ready, steady, go!

- 5 min to 9p.m. (Eindhoven time): all machines ready, waiting for dictionary.

Ready, steady, go!

- 5 min to 9p.m. (Eindhoven time): all machines ready, waiting for dictionary.
- Dictionary is out, words `ruby` and `tokyo` from test dictionary are contained.

Ready, steady, go!

- 5 min to 9p.m. (Eindhoven time): all machines ready, waiting for dictionary.
- Dictionary is out, words `ruby` and `tokyo` from test dictionary are contained.
- Quickly scanning dictionary we find more “fun” words `bugs` and `blank`

Ready, steady, go!

- 5 min to 9p.m. (Eindhoven time): all machines ready, waiting for dictionary.
- Dictionary is out, words `ruby` and `tokyo` from test dictionary are contained.
- Quickly scanning dictionary we find more “fun” words `bugs` and `blank`
- On way home find even nicer words `cows` and `dirty`.

Ready, steady, go!

- 5 min to 9p.m. (Eindhoven time): all machines ready, waiting for dictionary.
- Dictionary is out, words `ruby` and `tokyo` from test dictionary are contained.
- Quickly scanning dictionary we find more "fun" words `bugs` and `blank`
- On way home find even nicer words `cows` and `dirty`.
- Some set-backs:
  - 1 cluster machine too hot;
  - most powerful computers down in Taiwan;
  - still a few hours till Bo-Yin appears at work.
- We're stuck at distance 33 while someone else has already two! entries at distance 31.

Results

- By calling up a few good friends (with GPUs) one can get up to 3 billion SHA-1 hashes per second.
- GPUs are much more powerful on such computations than CPUs. Details are online.

Results

- By calling up a few good friends (with GPUs) one can get up to 3 billion SHA-1 hashes per second.
- GPUs are much more powerful on such computations than CPUs. Details are online.
- We got lucky – 1 entry at 31 and 1 entry at 30 – much better than estimated!

Results

- By calling up a few good friends (with GPUs) one can get up to 3 billion SHA-1 hashes per second.
- GPUs are much more powerful on such computations than CPUs. Details are online.
- We got lucky – 1 entry at 31 and 1 entry at 30 – much better than estimated!
- The phrase
  `BuGS bugs bUgs BUGs BLAnK BlAnK blANK BlaNK BuGS BUgS buGS bugS FkCjV`
  is useful!

Results

- By calling up a few good friends (with GPUs) one can get up to 3 billion SHA-1 hashes per second.
- GPUs are much more powerful on such computations than CPUs. Details are online.
- We got lucky – 1 entry at 31 and 1 entry at 30 – much better than estimated!
- The phrase
  `BuGS bugs bUgs BUGs BLAnK BlAnK blANK BlaNK BuGS BUgS buGS bugS FkCjV`
  is useful!
- Paul has now an iPhone and Doug some cloud credit.

Results

- By calling up a few good friends (with GPUs) one can get up to 3 billion SHA-1 hashes per second.
- GPUs are much more powerful on such computations than CPUs. Details are online.
- We got lucky – 1 entry at 31 and 1 entry at 30 – much better than estimated!
- The phrase
  `BuGS bugs bUgs BUGs BLAnK BlAnK blANK BlaNK BuGS BUgS buGS bugS FkCjV`
  is useful!
- Paul has now an iPhone and Doug some cloud credit.
- Dan got critical acclaim for his “OCD-like”
  `cOWs cOwS cOwS cowS DIRtY Dirty DiRTY DIrtY cOWS Cows CoWs Cows owjo0`

Aftermath

AL3X (Alex Payne, Twitter's Platform Lead) tweets:

`We've got a bunch of celebrities on Twitter, but I think @hashbreaker (djb) is our first deity`