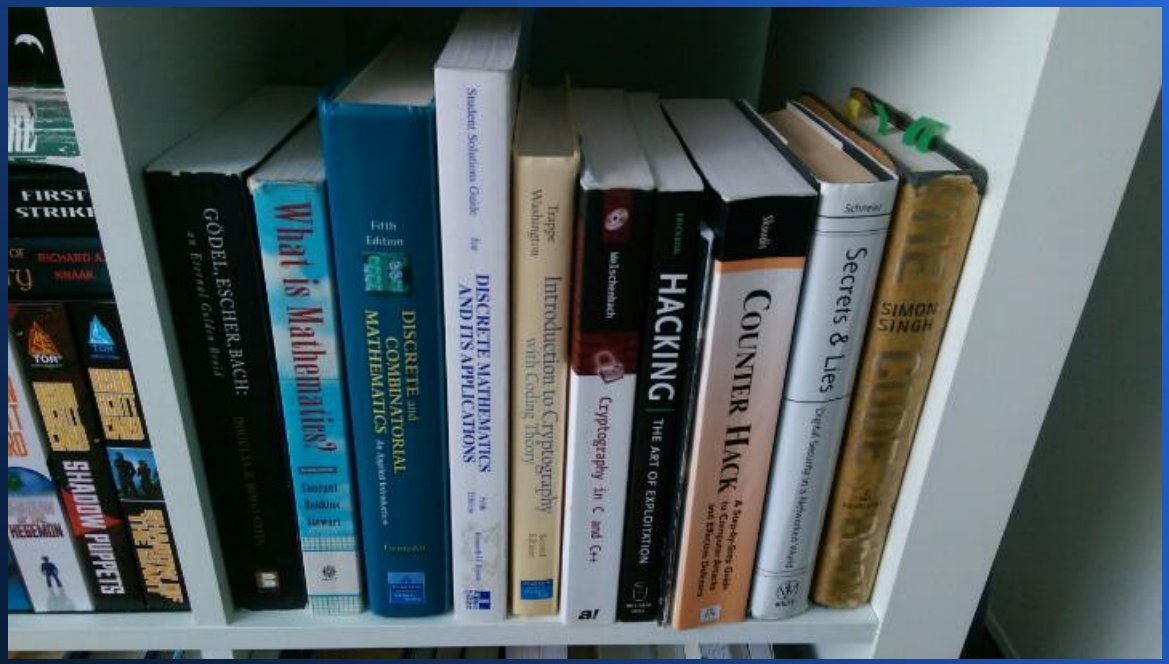
Cryptography for Game Dev



BlueLine
GAME STUDIOS

Before we get started...

- Slides: http://blgsi.com/ecgc2015

- Who we are – BlueLine Game Studios
- Purpose of the talk

BlueLine
GAME STUDIOS

Before we get started...

- Slides: http://blgsi.com/ecgc2015

- Who we are – BlueLine Game Studios
- Purpose of the talk

BlueLine
GAME STUDIOS

Table of Contents

1. Common Use-Cases
2. Solutions for Common Use-Cases
3. Which Algorithms are Considered Secure Today
4. Rules to Remember!

No math, but...

BlueLine GAME STUDIOS

Table of Contents

Interspersed Crypto Lessons! :D

BlueLine GAME STUDIOS

Common Game Dev Uses of Crypto

1. Great!
    1. User Accounts & Passwords
2. Not so reliable
    1. Semi-securely encrypting files
    2. Signing web-requests (sorta-reliable Highscores)
3. Completely Futile
    1. Trustworthy clients (reliable Highscores for $)
    2. Encrypted files for item-ownership

BlueLine GAME STUDIOS

Common Game Dev Uses of Crypto

1. Great!
    1. User Accounts & Passwords
2. Not so reliable
    1. Semi-securely encrypting files
    2. Signing web-requests (sorta-reliable Highscores)
3. Completely Futile
    1. Trustworthy clients (reliable Highscores for $)
    2. Encrypted files for item-ownership

BlueLine GAME STUDIOS

Accounts & Passwords

- Storing passwords securely (everyone)
  - Never store passwords, only store hashes.
  - … CRYPTO LESSON!
- Transmitting passwords (valuable accounts)

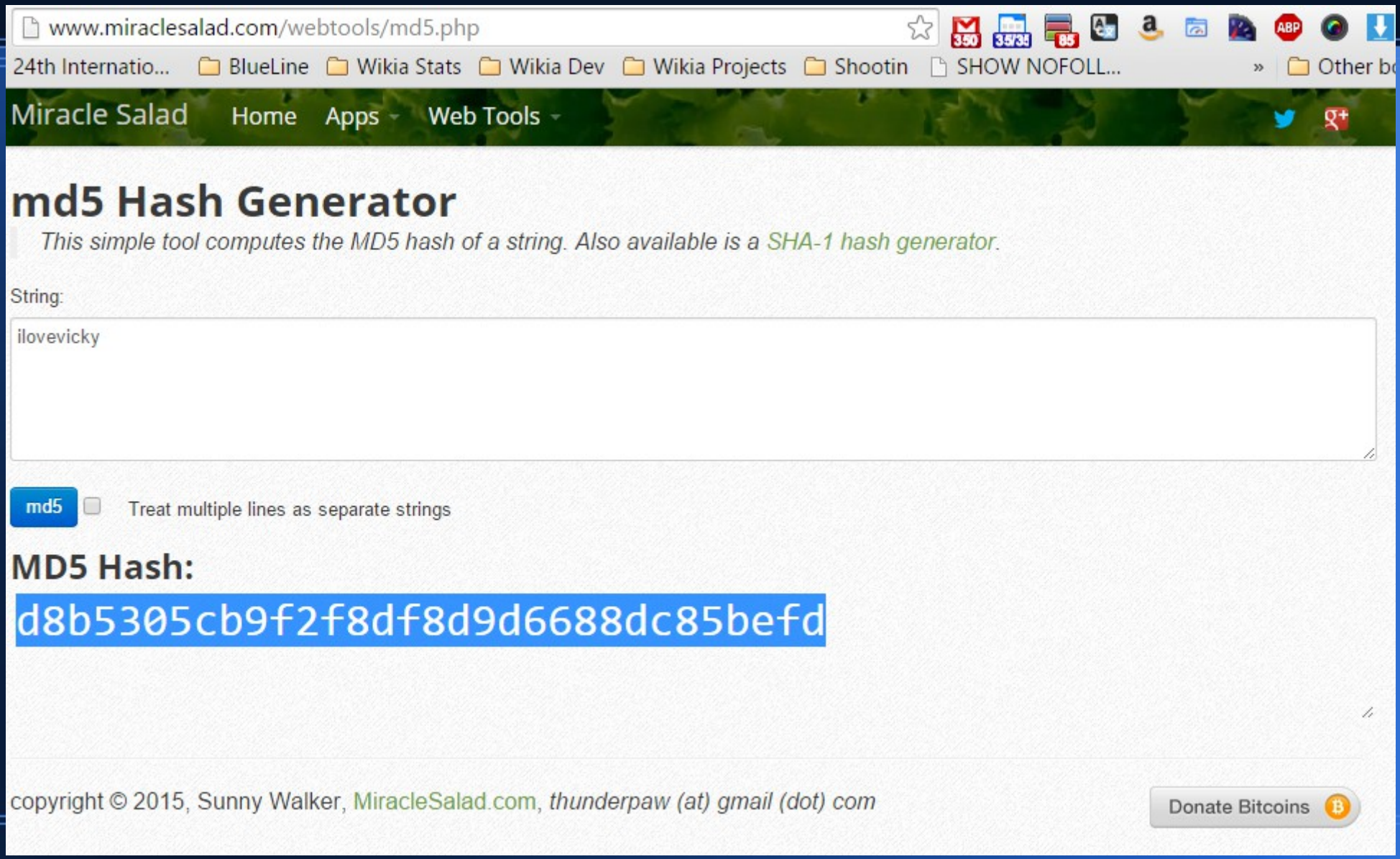
Crypto Lesson #1: Hashes

- String that is easy to go from A → B, hard to go back from B → A.

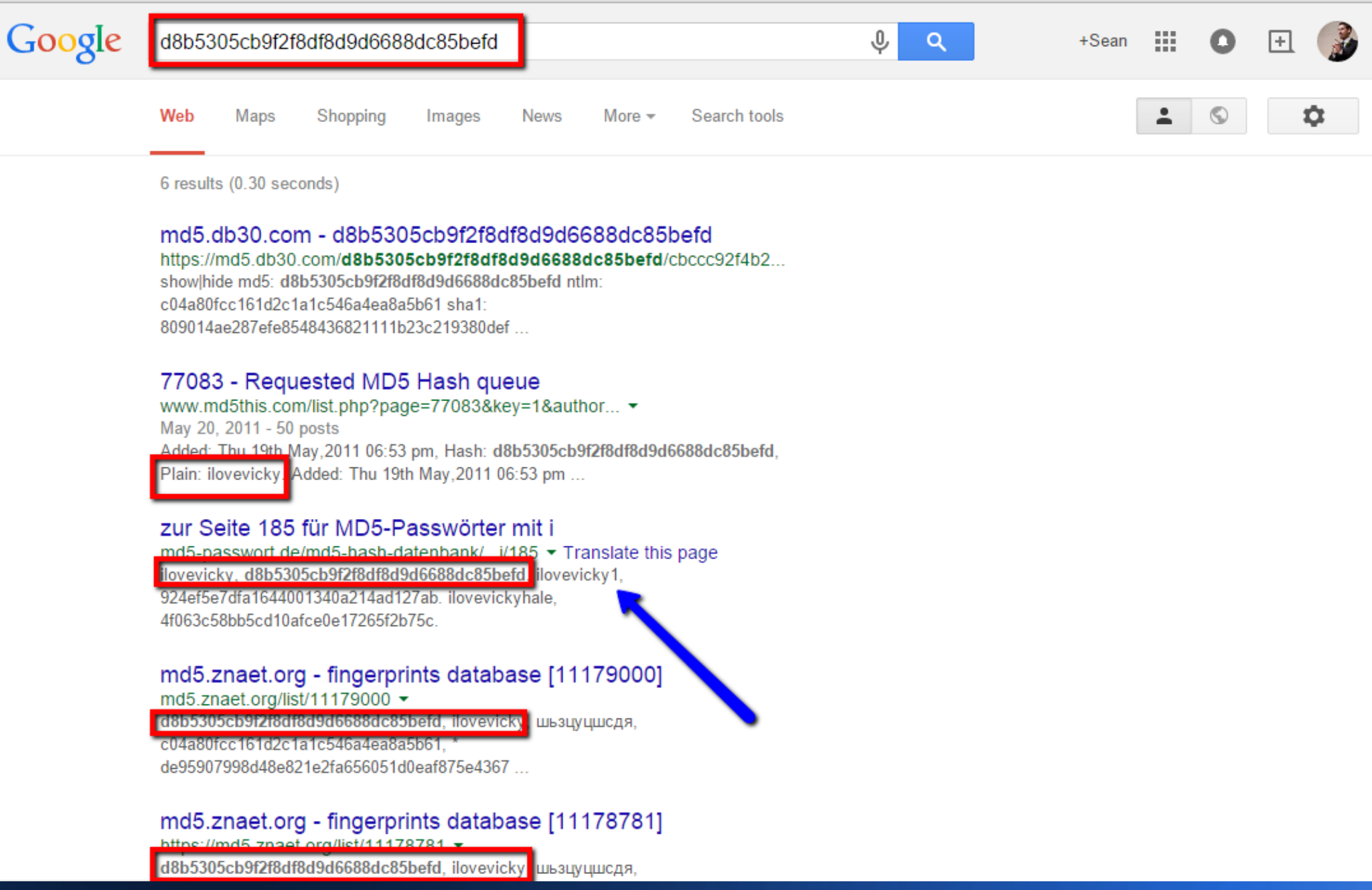
  md5(bob) → 9f9d51bc70ef21ca5c14f307980a29d8

- Collisions – don't need actual “A” just something that collides A → B and Q → B
- md5 isn't great anymore...

md5


www.miraclesalad.com/webtools/md5.php
24th Internatio...
BlueLine
Wikia Stats
Wikia Dev
Wikia Projects
Shootin
SHOW NOFOLL...
Other b
Miracle Salad
Home
Apps
Web Tools
md5 Hash Generator
This simple tool computes the MD5 hash of a string. Also available is a SHA-1 hash generator.
String:
ilovevicky
md5
Treat multiple lines as separate strings
MD5 Hash:
d8b5305cb9f2f8df8d9d6688dc85befd
copyright © 2015, Sunny Walker, MiracleSalad.com, thunderpaw (at) gmail (dot) com
Donate Bitcoins

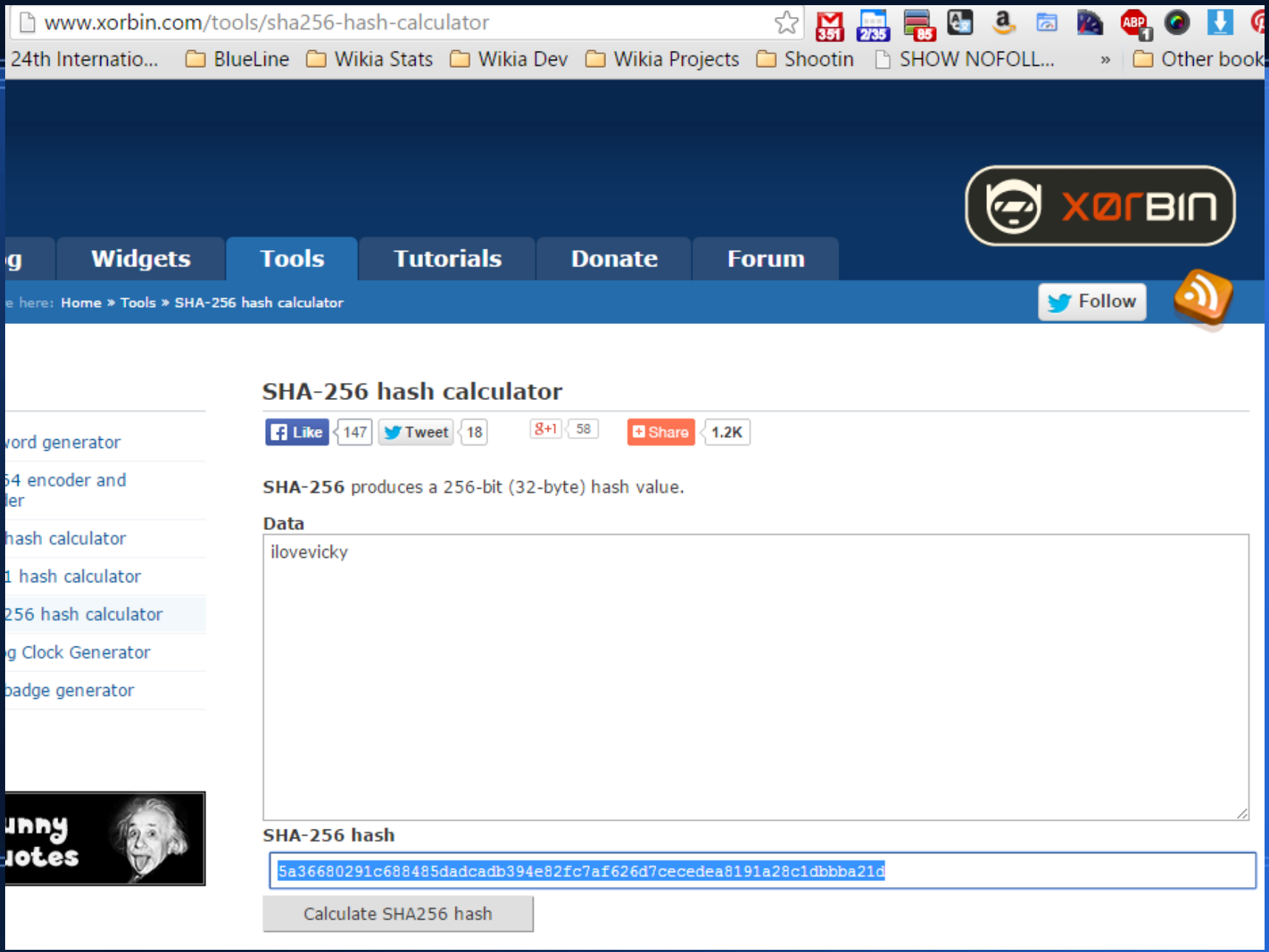
md5


Google
d8b5305cb9f2f8df8d9d6688dc85befd
+Sean
Web
Maps
Shopping
Images
News
More
Search tools
6 results (0.30 seconds)
md5.db30.com - d8b5305cb9f2f8df8d9d6688dc85befd
https://md5.db30.com/d8b5305cb9f2f8df8d9d6688dc85befd/cbccc92f4b2...
show|hide md5: d8b5305cb9f2f8df8d9d6688dc85befd ntlm:
c04a80fcc161d2c1a1c546a4ea8a5b61 sha1:
809014ae287efe8548436821111b23c219380def ...
77083 - Requested MD5 Hash queue
www.md5this.com/list.php?page=77083&key=1&author...
May 20, 2011 - 50 posts
Added: Thu 19th May,2011 06:53 pm, Hash: d8b5305cb9f2f8df8d9d6688dc85befd,
Plain: ilovevicky. Added: Thu 19th May,2011 06:53 pm ...
zur Seite 185 für MD5-Passwörter mit i
md5-passwort.de/md5-hash-datenbank/...i/185
Translate this page
ilovevicky, d8b5305cb9f2f8df8d9d6688dc85befd, ilovevicky1,
924ef5e7dfa1644001340a214ad127ab, ilovevickyhale,
4f063c58bb5cd10afce0e17265f2b75c.
md5.znaet.org - fingerprints database [11179000]
md5.znaet.org/list/11179000
d8b5305cb9f2f8df8d9d6688dc85befd, ilovevicky, шьзцучшсдя,
c04a80fcc161d2c1a1c546a4ea8a5b61, *
de95907998d48e821e2fa656051d0eaf875e4367 ...
md5.znaet.org - fingerprints database [11178781]
https://md5.znaet.org/list/11178781
d8b5305cb9f2f8df8d9d6688dc85befd, ilovevicky, шьзцучшсдя,

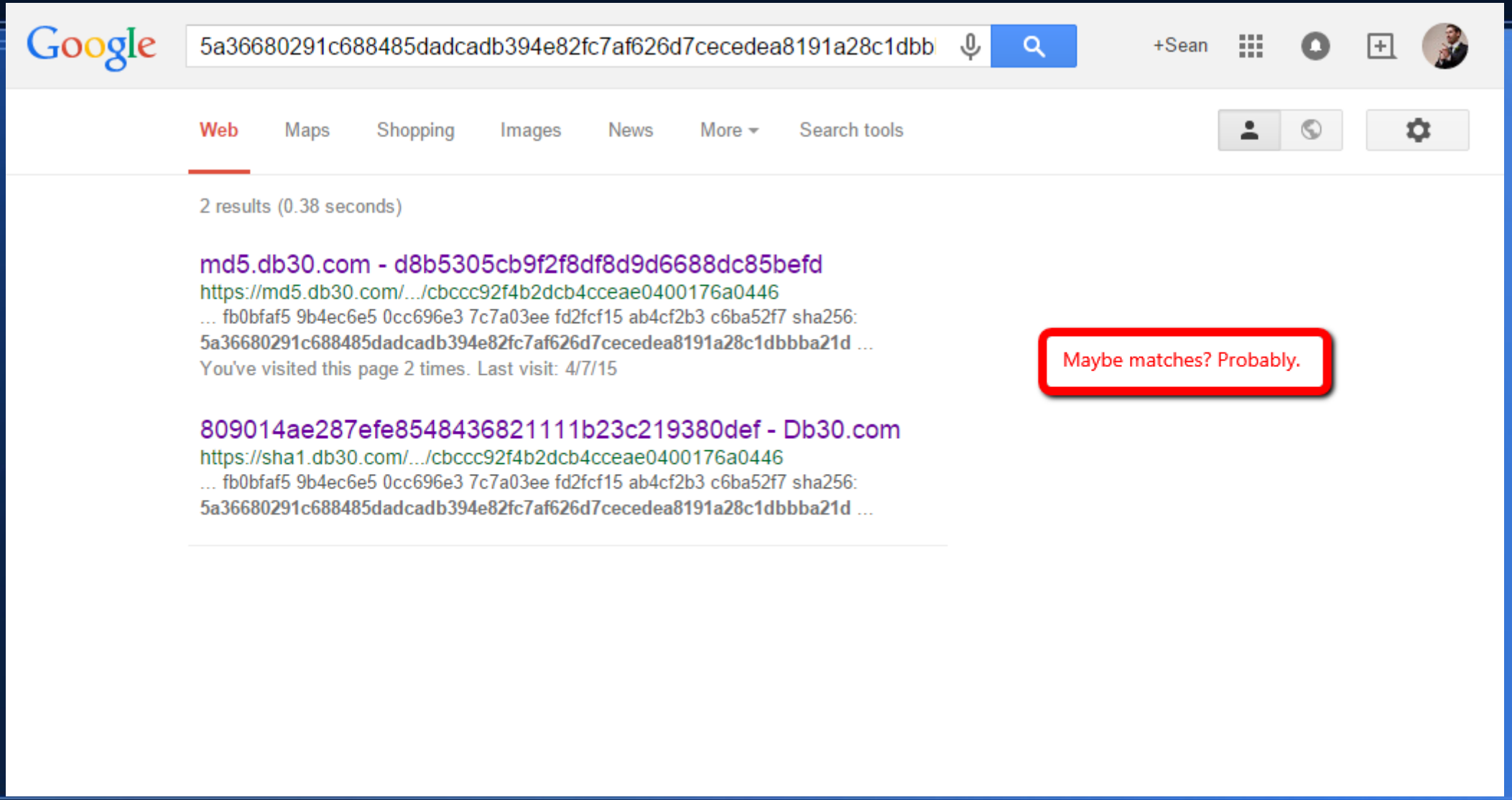
Crypto Lesson #1: Hashes

- String that is easy to go from A → B, hard to go back from B → A.
- Collisions – don't need actual “A” just something that collides
- md5 isn't great anymore
- SALT YO HASHES!
  - hash(“bob”) → “1cwY”, hash(“1cwY” + “bob”)
  - Per-password, not per system...

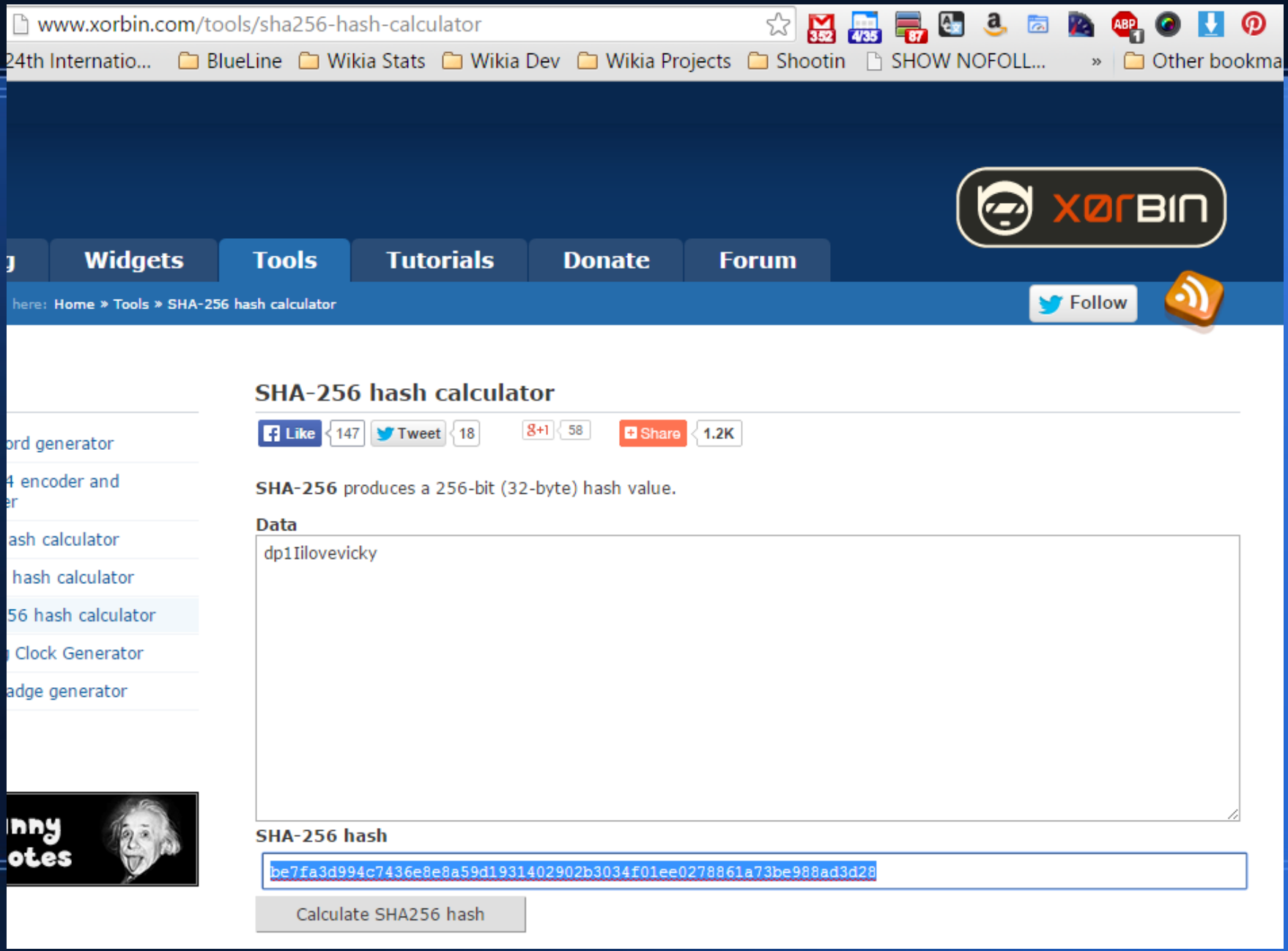
sha256


www.xorbin.com/tools/sha256-hash-calculator
24th Internatio...
BlueLine
Wikia Stats
Wikia Dev
Wikia Projects
Shootin
SHOW NOFOLL...
Other book
XORBIN
Widgets
Tools
Tutorials
Donate
Forum
Home » Tools » SHA-256 hash calculator
Follow
SHA-256 hash calculator
Like 147
Tweet 18
58
Share 1.2K
SHA-256 produces a 256-bit (32-byte) hash value.
Data
ilovevicky
SHA-256 hash
5a36680291c688485dadcadb394e82fc7af626d7cecedea8191a28c1dbbba21d
Calculate SHA256 hash

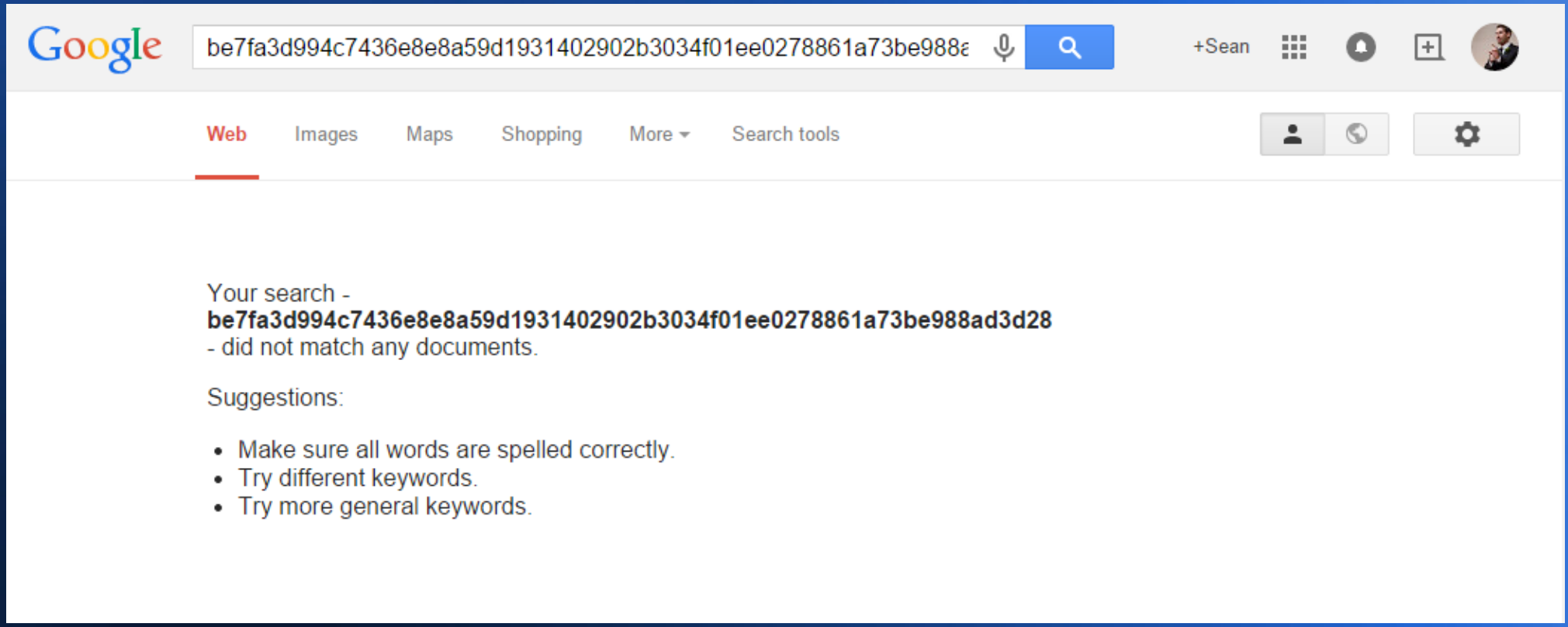
sha256


Google
5a36680291c688485dadcadb394e82fc7af626d7cecedea8191a28c1dbb
+Sean
Web
Maps
Shopping
Images
News
More
Search tools
2 results (0.38 seconds)
md5.db30.com - d8b5305cb9f2f8df8d9d6688dc85befd
https://md5.db30.com/.../cbccc92f4b2dcb4cceae0400176a0446
... fb0bfaf5 9b4ec6e5 0cc696e3 7c7a03ee fd2fcf15 ab4cf2b3 c6ba52f7 sha256:
5a36680291c688485dadcadb394e82fc7af626d7cecedea8191a28c1dbbba21d ...
You've visited this page 2 times. Last visit: 4/7/15
809014ae287efe85484368211111b23c219380def - Db30.com
https://sha1.db30.com/.../cbccc92f4b2dcb4cceae0400176a0446
... fb0bfaf5 9b4ec6e5 0cc696e3 7c7a03ee fd2fcf15 ab4cf2b3 c6ba52f7 sha256:
5a36680291c688485dadcadb394e82fc7af626d7cecedea8191a28c1dbbba21d ...
Maybe matches? Probably.

sha256 - salted



sha256 - salted



Crypto Lesson #1: Hashes

- String that is easy to go from A → B, hard to go back from B → A.
- Collisions – don't need actual “A” just something that collides
- md5 isn't great anymore
- SALT YO HASHES!
  - hash(“bob”) → “1cwY”, hash(“1cwY” + “bob”)
  - Per-password, not per system.

- Search “password storage cheat sheet”

Accounts & Passwords

- Storing passwords securely (everyone)
  - Never store passwords, only store hashes/salts.
- Transmitting passwords (valuable accounts)
  - HTTPS (SSL/TLS)

Common Game Dev Uses of Crypto

1. Great!
    1. User Accounts & Passwords
2. Not so reliable
    1. Semi-securely encrypting files
    2. Signing web-requests (sorta-reliable Highscores)
3. Completely Futile
    1. Trustworthy clients (reliable Highscores for $)
    2. Encrypted files for item-ownership

BlueLine GAME STUDIOS

Meh: Encrypting Files

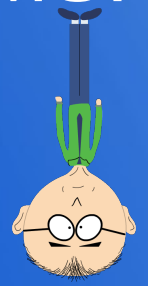
- Possible use: unlocking important DLC (eg: in a deck-building game).
- Why it doesn't work ...CRYPTO LESSON!

Crypto Lesson #2: What Works!

- DON'T INVENT YOUR OWN ALGORITHMS!
  - 10,000s of hours
  - Security By Obscurity... is bad, mkay?
  - Most languages have these done already
- Only known provably secure crypto is “One Time Pad”s (except Quantum Crypto)
  - Private keys
  - Use once & discard

Crypto Lesson #2: What Works!

- DON'T INVENT YOUR OWN ALGORITHMS!
  - 10,000s of hours
  - Security By Obscurity... is bad, mkay?
  - Most languages have these done already



- Only known provably secure crypto is “One Time Pad”s (except Quantum Crypto)
  - Private keys
  - Use once & discard
- LESSON COMPLETE! \m/

Meh: Encrypting Files

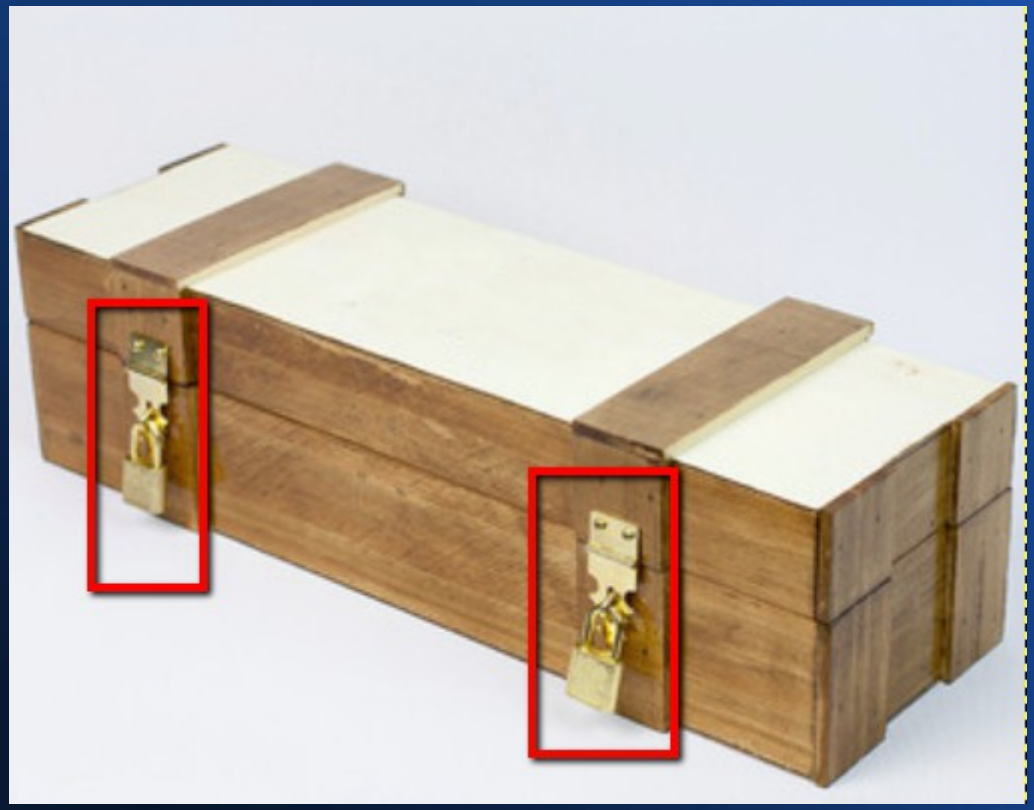
- Possible use: unlocking important DLC (eg: in a deck-building game).
- Why it doesn't work (private key in code)
- Keeps people from manually messing with files *easily*.
- ...but not dependable.
- Crypto is not the answer here (use an server)

Meh: Signing Web Requests

- Possible use: reporting High Scores securely
- Signatures ...but first, CRYPTO LESSON!!

Crypto Lesson #3: Public Key Crypto

- Diffie Hellman Key Exchange



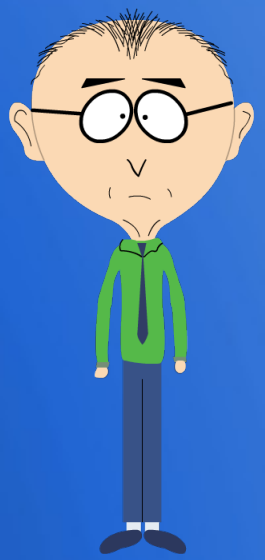
Crypto Lesson #3: Public Key Crypto

- Diffie Hellman Key Exchange
- RSA, etc.

source

Crypto Lesson #3: Public Key Crypto

- Diffie Hellman Key Exchange
- RSA, etc.
- The math is complicated
  - RSA Factoring Challenge
  - Large Prime Products are hard to factor (mkay?)
    - …unless you have quantum computers.
      - I spent years working on this. Sqrt() faster :/
- Often used to just exchange keys for 1TimePad



Crypto Lesson #3: Public Key Crypto

- Diffie Hellman Key Exchange
- RSA, etc.
- The math is complicated
  - RSA Factoring Challenge
  - Large Prime Products are hard to factor (mkay?)

    …unless you have quantum computers.
    - I spent years working on this. Sqrt() faster :/
- Often used to just exchange keys for 1TimePad

LESSON COMPLETE! \m/

Meh: Signing Web Requests

- Possible use: reporting High Scores securely
- Signatures
  - Structure & code...

Meh: Signing Web Requests

- NORMAL: [data]
- SIGNED: [data]+[signature from data]
- ...

Meh: Signing Web Requests

- NORMAL: [data]
- SIGNED: [data]+[signature from data]
- BONUS: [data]+[salt]+[signature of salty data]
  - Only really needed if “data” is going to be used repeatedly. Like... “buy a mudkip”.
  - Prevents replay-attacks (salt must be a nonce)

Meh: Signing Web Requests

```
/// <summary>
/// Given a data-string for a a request, returns a signed version of that string. This will
/// be used on the server-side to verify that this request came from one of our
/// games.
///
/// Refer to cryptoTools.php for more details on the signature scheme.
///
/// Basically this signature is just a hash of the "hashedData" with a secret
/// token pre-pended. The server also has a copy of this secret token.
/// </summary>
/// <param name="hashedData"></param>
private string GetSignatureForSortedDataString(string dataString)
{
    SHA256 hashTool = SHA256Managed.Create();

    // The data to hash is just the request's 'hashedData' with a secret token prepended.
    string dataToHash = SHARED_TOKEN + dataString;

    byte[] signatureBytes = hashTool.ComputeHash(Encoding.UTF8.GetBytes(dataToHash));
    StringBuilder sigStringBuilder = new StringBuilder();
    for (int index = 0; index < signatureBytes.Length; index++)
    {
        sigStringBuilder.Append( String.Format("{0:x2}", signatureBytes[index]) );
    }

    return sigStringBuilder.ToString();
}
```

Meh: Signing Web Requests

- Possible use: reporting High Scores securely
- Signatures
  - Structure & code
- Why it doesn't work (private key in code)
- Will make it take longer before your highscores get hacked. But they will.

Common Game Dev Uses of Crypto

1. Great!
    1. User Accounts & Passwords
2. Not so reliable
    1. Semi-securely encrypting files
    2. Signing web-requests (sorta-reliable Highscores)
3. Completely Futile
    1. Trustworthy clients (reliable Highscores for $)
    2. Encrypted files for item-ownership

BlueLine GAME STUDIOS

Table of Contents

BlueLine
GAME STUDIOS

Algorithms of Today

- Public Key Crypto
  - RSA / PGP
  - HTTPS (SSL/TLS)
- Hashes
  - md5 is outdated for security purposes!
  - sha256 is sha2
    - Getting more popular than sha1 (kinda bad.. mkay)
  - SALT YO HASHES!

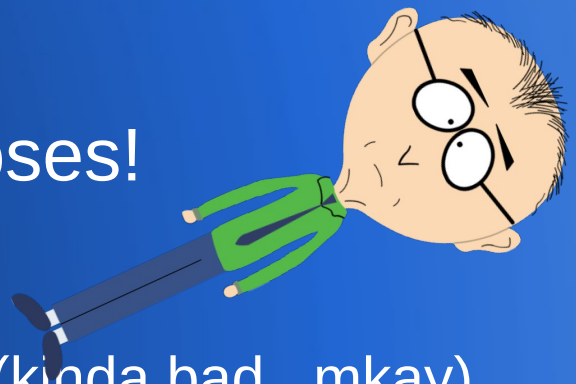


Table of Contents

BlueLine
GAME STUDIOS

Rules to Remember!!

1. Don't invent your own algorithms!
2. You will almost never have to even IMPLEMENT the algorithms, just use them from libraries!
3. SALT YO HASHES!
4. Clients lie. Don't believe the clients' Lies!

source

Table of Contents

BlueLine
GAME STUDIOS

QUESTIONS?

- Download this whole presentation online!
  - http://blgsi.com/ecgc2015
- Visit our booth at ECGC 2015! :)
- If you have more questions later:
  - http://twitter.com/BlueLineGames
  - http://BlueLineGameStudios.com

BlueLine
GAME STUDIOS