javascript crypto.

ugly duckling with good reason?

a freelancer,
like him

concerned about security, like them

love ruby,
not like him

„so what are
you doing at
jsconf ?“

i love crypto

i love javascript, too

wrote a lot of java crypto code on the job wrote a lot of ruby & c

crypto code, too

never wrote any javascript crypto code

why?

javascript cryptography

considered harmful

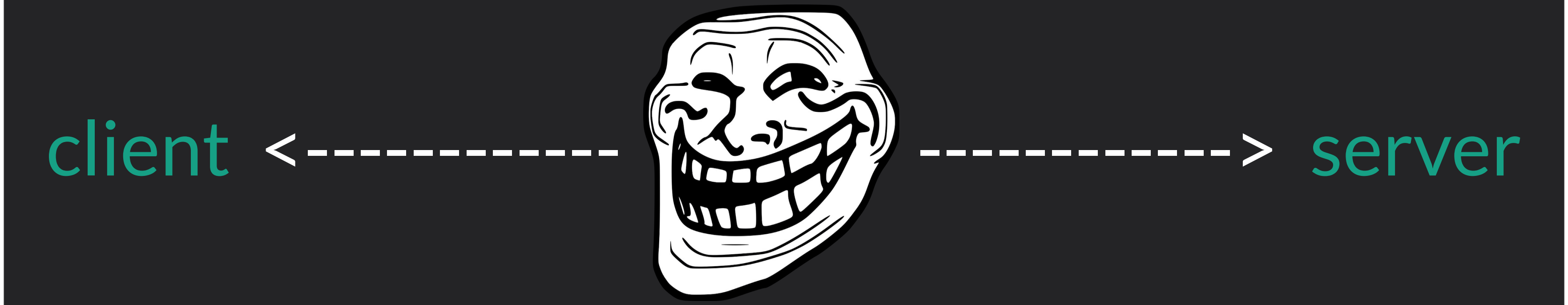
http://www.matasano.com/articles/javascript-cryptography/

!!! client-side !!!

let's see why it's doomed

js served over http

man-in-the-middle attack



client <------------- -------------> server serve different files

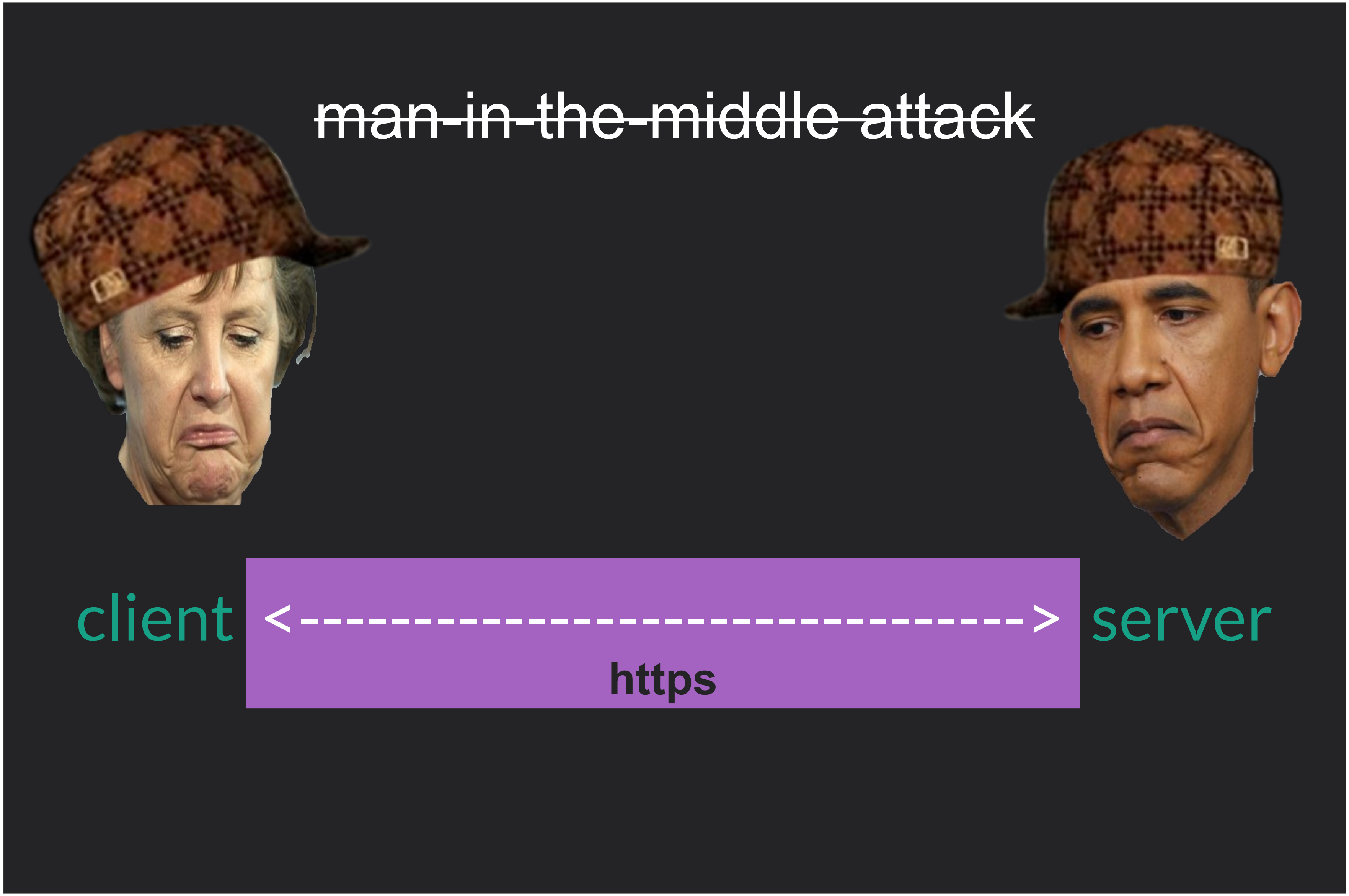
alter files on the fly

inject <script> tags

etc.

alright, let's take care of the network

https



~~man-in-the-middle attack~~

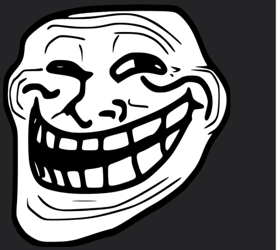
client

https

server

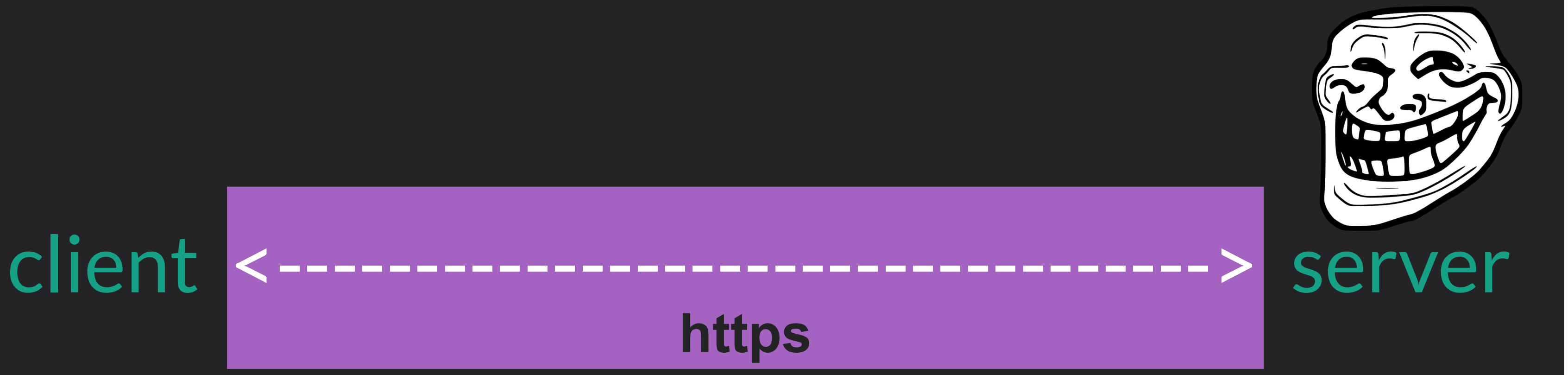
mission accomplished ?

man-on-the-server attack



client <-----------------------------------> server

works with https, too



client <-----------------------------------> server

https

if you don't trust apps to do

crypto for you

how could you trust their js crypto code?

note:

not a javascript problem per se

tho there are javascript problems as well often algorithms require

exact-width integer operations
(e.g. on 8 bit, 32 or 64 bit)

no out-of-the-box support

for binary data

no out-of-the-box support

for big integers

-> workarounds lack native support

-> workarounds are slow

then: browser js problems

lack of a universally supported

„cryptographically secure
pseudo-random
number generator“

(aka csprng)

Math.random is predictable

csprng is at the heart of crypto

without it, crypto === lulzcrypto

workarounds using mouse movement

and whatnot

meh

clearly something that should be built-in

```
window.crypto.getRandomValues
```

lacks wide-spread support

what makes javascript fun

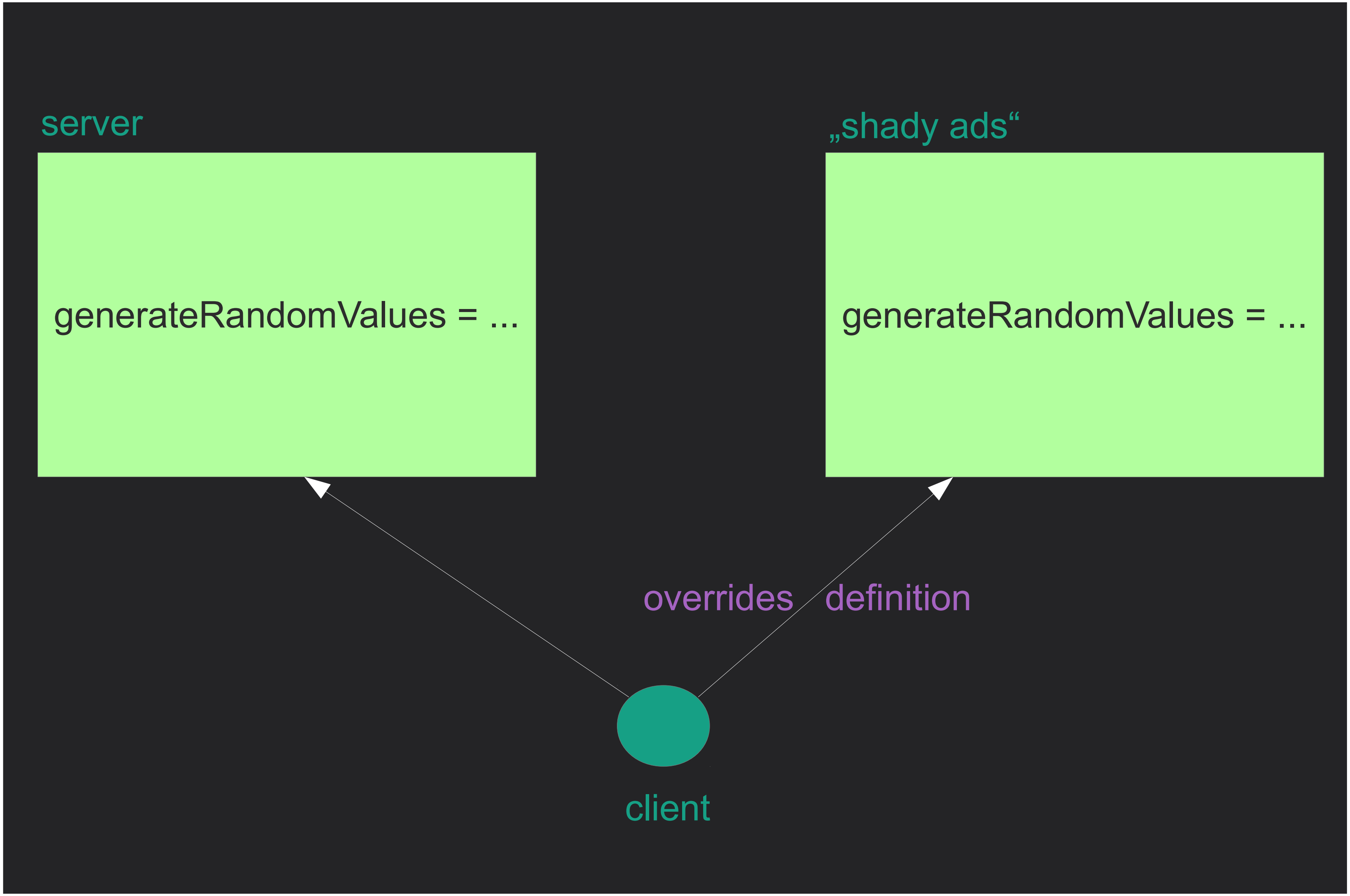
is also what makes javascript crypto hard dynamic runtime environment

```
crypto.generateRandomValues = function(array) {
   array[0] = 42;
};
```

doesn't even have to be intentional

```
/**
 * FTFY. Achieved web scale performance.
 */
crypto.encrypt = function(key, value) {
   /* military-grade ROT26 algorithm */
   return value;
};
```

javascriptcrypto



environment could be changing continuously

„so javascript crypto sucks,
end of story?“

a new hope

widely-adopted
browser-built-in

crypto functionality

asm.js

exact-width integer types

== typed array support

(http://www.khronos.org/registry/typedarray/specs/latest/)

w3c web cryptography api

biginteger support

built-in csprng

lots of good stuff

„dude, could you
finally get to the point
where you tell us
why we need crypto to begin with?
i never wrote any crypto code
and i certainly don't intend to."

privacy

„if you have

nothing to hide,

you have nothing to fear.“

bullshit

everyone has secrets

often embarrassing

if they were public knowledge

people forgive, but the internet does not today's surveillance is like radiation

while our governments may be

„benevolent in general“

it's individuals that do harm

not the government or „the system“ is evil people are evil

they will abuse their power

a series of well-intended myopic decisions may lead to something

escaping our control

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

even if companies provide perfect crypto they store data in plain text

ready for agencies to pick up

„what can we as individuals
do to protect our data?“

encrypt shit

on the client

-> gonna need client-side crypto

institutions may have leverage

over a single corp

but not over a billion individuals

„so what – i really
have nothing to hide.
just let them have it.“

surveillance

will tremendously change our lives

innocent until proven guilty

becomes

guilty until proven innocent

determinism

automated profiling

we are more than
a physical appearance
plus
the sum of our actions

„let them have my bikini pictures – i couldn't care less!“

people in memes are real people

surveillance throughout history

always „for the greater good“

(except that it's not)

not a single person felt safer

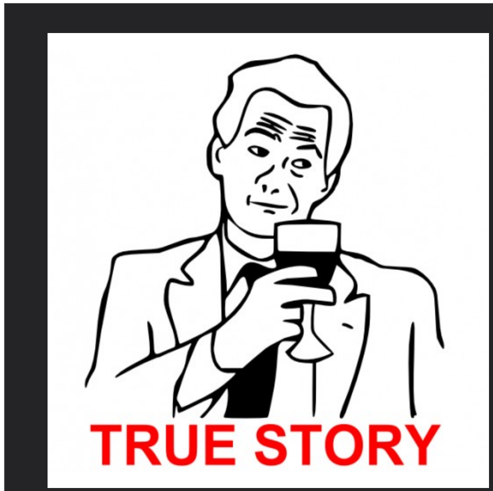
people were in constant fear

you will be told that

protecting yourself with crypto is bad

while agencies need it

badly to protect you



child molesters
human traffickers
drug lords
bla bla bla

we are supposed to have nothing to hide

while it's ok for agencies to have secrets

mutual trust

is security

more important than

personal freedom?

there is no security without it

the holy grail. homomorphic encryption.

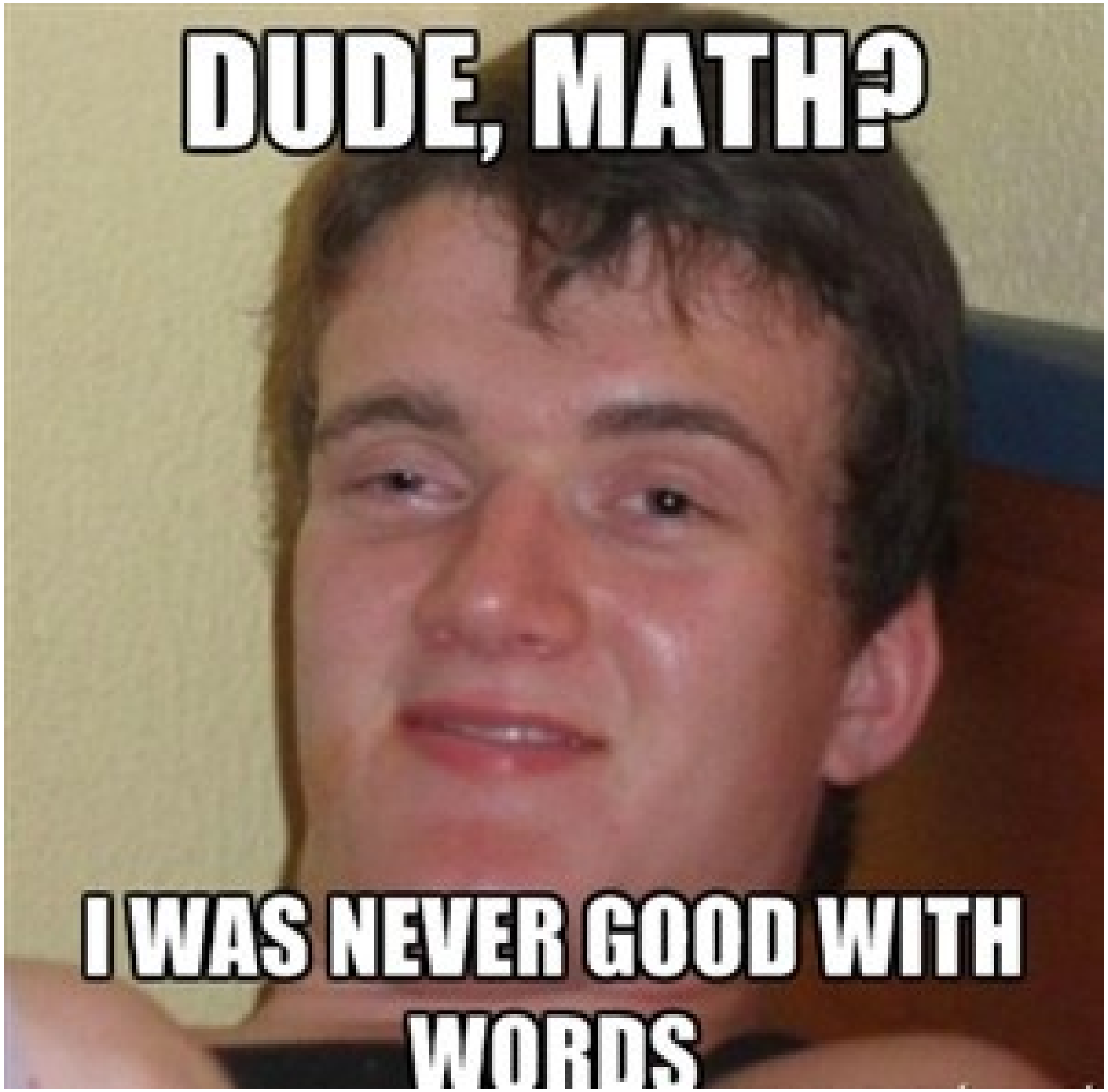
homomorphism

$f: (G,*) \rightarrow (H,*')$

such that

$f(g1 * g2) = f(g1) *' f(g2)$

for any elements $g1, g2 \in G$.


DUDE, MATH?
I WAS NEVER GOOD WITH WORDS

$f(x) := 1/x$

G, H := real numbers

*, *' := multiplication

$$f(a * b)$$

$$= 1 / (a *b)$$

$$= 1/a * 1/b$$

$$= f(a) *' f(b)$$

rsa

public key e

modulus m

encryption $E(x) := x^e \bmod m$

$$E(x1 * x2)$$

$$= (x1 * x2)^e \bmod m$$

$$= x1^e * x2^e \bmod m$$

$$= x1^e \bmod m * x2^e \bmod m$$

$$= E(x1) * E(x2)$$

but

E(x1+x2)

= (x1+x2)^e mod m

~~= x1^e + x2^e mod m~~

relatively easy to find

homomorphisms

for one of the two operations

homomorphism in both operations:

fully homomorphic encryption

$$f: (G,+,*) \rightarrow (H,+',*')$$

such that

$$f(g1 * g2) = f(g1) *' f(g2)$$

and

$$f(g1 + g2) = f(g1) +' f(g2)$$

for any elements g1, g2 ∈ G.

why is this so desirable?

it preserves the ring structure, that's why!

layman terms:

perform algorithms
on
encrypted data

think:

google executes your search
and returns the correct result
without learning anything
about your search term
or the result

yay, porn

holy grail of privacy

craig gentry

(http://www.americanscientist.org/issues/pub/2012/5/alice-and-bob-in-cipherspace)

„ok, cool story, bro,
but would you mind
telling us what we can
do right now?“

european eid cards

great in theory

„martin, i just got a call
from the 90s – they said
they finally wanted their
java applets back.“

firefox

```
signText(stringToSign, caOption, ...)
```

please, browser people

pkcs#11 support

-> out-of-band keys

with strong protection

we as developers must fix the problem

pgp
s/mime
client-side encryption tools

how often did your mom use them lately?

opt-in ain't gonna work

what we need is implicit

security by default

academia must fix the problem

sharing schemes

that render extortion useless

„one-time encryption“

(like the notes in mission impossible)

use w3c web crypto api

major step forward

„wait a minute -
didn't you say that we
cannot trust js code
anyway? so how is the
w3c api gonna help?!“

it all boils down to trust

at some point, you need to trust

thinking this further:

how do you know

any of your software is authentic and/or benevolent?

chicken & egg

https download/verifying signature ->

need software for that ->

infinite recursion

still, major improvement

because apps cannot access secrets

but:

encrypting data with aes

```
var data = „Le secret“;
var clearDataArrayBufferView = convertPlainTextToArrayBufferView(data);

var aesAlgorithmKeyGen = {
  name: "AES-CBC",
  params: { length: 128 }
};

var aesAlgorithmEncrypt = {
  name: "AES-CBC",
  params: { iv: window.crypto.getRandomValues(new Uint8Array(16)) }
};

var cryptoKeyGen = window.crypto.generateKey(aesAlgorithmKeyGen,
                                             false,
                                             ["encrypt"]);

cryptoKeyGen.oncomplete = function(event) {
  var aesKey = event.target.result;
  var aesOp = window.crypto.encrypt(aesAlgorithmEncrypt,
                                    aesKey,
                                    clearDataArrayBufferView);
  aesOp.oncomplete = function(event) {
    var ciphertext = event.target.result;
  };
  aesOp.onerror = function(event) { console.error("Unable to encrypt."); };
};
```

o_O

low-level api in the tradition of openssl with full control

but also full possibility to hang yourself no secure defaults

what i want is this

javascriptcrypto

```
var data = „Le secret“;
var key = window.crypto.generateKey();
var encrypted = window.crypto.encrypt(key, data);
/* nuff said */
```

crypto is hard, sure

but do crypto apis have to be, too?

krypt. semper pi.

ruby framework that wraps expert apis™

to make crypto accessible for human beings so how would you like the sound of

KRYPT
Platform- and library-independent cryptography for Ruby
SEMPER
Π

krypt.js

thank you

https://github.com/krypt

http://martinbosslet.de

martin.bosslet@gmail.com

@_emboss_