Melissa Lynn

University of Minnesota

Password Security

How do websites store passwords?
Why do they require me to include three different types of characters?
What makes a good password?
What could happen if something goes wrong in this process?

SURVEY

Raise your hand if you use the same password for multiple accounts.

SURVEY

Raise your hand if your password consists of a single english word, plus some numbers and/or symbols.

SURVEY

Raise your hand if you use a password manager.

Password Security

How do websites store passwords?
Why do they require me to include three different types of characters?
What makes a good password?
What could happen if something goes wrong in this process?

Password security relies on an important tool in cryptology: a special type of one-way function called a cryptographic hash function.
We will talk about how and why these functions are used in password storage, as well as what can go wrong if they aren't used correctly.

Question:

Why shouldn't companies store a table of users' passwords to verify against when someone tries to log in?

Question:

Why shouldn't companies store a table of users' passwords to verify against when someone tries to log in?

- If a hacker obtains that table, they can immediately access all accounts.
- Furthermore, if a user has the same passwords across multiple sites, their other accounts are vulnerable as well.

Cryptographic hash functions provide a solution!

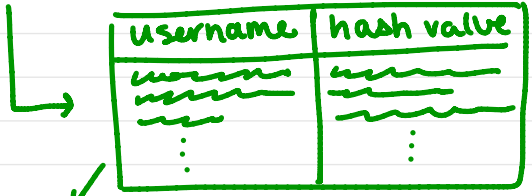
Idea: We'll apply a "one-way" function, and store the value of that function instead!

User enters their password: password1

Computer applies function: SHA-1

E38AD214943DAAD1D64C102FAEC29DE4AFE9DA3D

Computer checks this against table of hash values:



If it matches, you're logged in: SUCCESS!

The type of function that achieves this is called a cryptographic hash function.

Properties of a good CHF:

- Output has fixed size
- deterministic - same password always results in the same hash value
- quick to compute (but not too quick)
- preimage resistance - difficult to determine input from output except by trying all possible inputs.
- collision resistance - difficult to find two inputs that give the same hash value output.
- small change to input results in large change to output (appears random)

Question Why are each of these desirable?

Attacking a Hash Function

Andy [redacted] ▶ Melissa Lynn
November 23, 2013 ·

A lesson in cryptography:

This is the sha1 function applied to your nickname. Inverting this function is algorithmically difficult. When you learn your nickname, you can apply the sha1 function to it and verify that I know your nickname.

Your nickname: 6745faafad9f0583c626e21338da8227399efd34
But it should have been: ae7481973e6c9f63ea91e7cd1b77d8821b8e072d

Melissa Lynn You did know it! Now what is the should-have-been? (Other than nowhere near as awesome as Athena)

December 8, 2013 at 5:26pm · Like

Melissa Lynn nm I got it. Athena is way better than Turbo. You're lucky I didn't put effort into this, or I would have used this two weeks ago: http://reverse-hash-lookup.online-domain-tools.com/

> **Reverse Hash Lookup - Reveal plaintext from MD5/SHA1 hashes**
>
> Tries to reveal the original plaintext messages from specified hash values of several cryptographic hash functions.
>
> REVERSE-HASH-LOOKUP.ONLINE-DOMAIN-TOOLS.COM

December 8, 2013 at 5:29pm · Like · Remove Preview

Geoff [redacted] Da[redacted]n it Andy. You're really bad at keeping secrets.

December 8, 2013 at 5:37pm · Unlike · 1

Andy [redacted] this is ridiculous. this website literally has a database of all the possible values you might plug it. i should have applied it twice. well, i've definitely changed my mind in the past few weeks. athena is much cooler.

December 8, 2013 at 6:59pm · Unlike · 1

Jed [redacted] For this reason, using a common hash function without salt does not make a very good commitment scheme.

December 8, 2013 at 6:59pm · Like

Melissa Lynn A lesson in cryptography: Melissa > cryptography

December 8, 2013 at 11:23pm · Like · 1

Attacking a Hash Function

- Apply the function to common words and store the hash values.
- This is called a Rainbow Attack.

How to protect against it:

- Apply the hash function multiple times
- Add some extra nonsense characters to your input (salt)

- When storing passwords, the hash values are stored with the salt (different salt for each person)

HACKERS RECENTLY LEAKED **153 MILLION** ADOBE USER EMAILS, ENCRYPTED PASSWORDS, AND PASSWORD HINTS.

ADOBE ENCRYPTED THE PASSWORDS IMPROPERLY, MISUSING BLOCK-MODE 3DES. THE RESULT IS SOMETHING WONDERFUL:

USER PASSWORD		HINT
4e18acc1ab27a2d6		WEATHER VANE SWORD
4e18acc1ab27a2d6		
4e18acc1ab27a2d6	a0a2876eb1ea1fca	NAME 1
8babb6299e06eb6d		DUH
8babb6299e06eb6d	a0a2876eb1ea1fca	
8babb6299e06eb6d	85e9da81a8a78adc	57
4e18acc1ab27a2d6		FAVORITE OF 12 APOSTLES
1ab29ae86da6e5ca	7a2d6a0a2876eb1e	WITH YOUR OWN HAND YOU HAVE DONE ALL THIS
a1f9b2b6299e7a2b	eadec1e6ab797397	SEXY EARLOBES
a1f9b2b6299e7a2b	617ab0277727ad85	BEST TOS EPISODE
39738b7adb0b8af7	617ab0277727ad85	SUGARLAND
1ab29ae86da6e5ca		NAME + JERSEY #
877ab7889d3862b1		ALPHA
877ab7889d3862b1		
877ab7889d3862b1		
877ab7889d3862b1		OBVIOUS
877ab7889d3862b1		MICHAEL JACKSON
38a7c9279cadeb44	9dca1d79d4dec6d5	
38a7c9279cadeb44	9dca1d79d4dec6d5	HE DID THE MASH, HE DID THE
38a7c9279cadeb44		PURLOINED
a8ae5745a2b7af7a	9dca1d79d4dec6d5	FAV WATER-3 POKEMON

THE GREATEST CROSSWORD PUZZLE IN THE HISTORY OF THE WORLD

Question What can you do to keep your password secure?

Question What can you do to keep your password secure?

- don't use english words in your password
- use special symbols and numbers
- have a long password
- don't use the same password on multiple sites
- don't use password hints

Take the password:

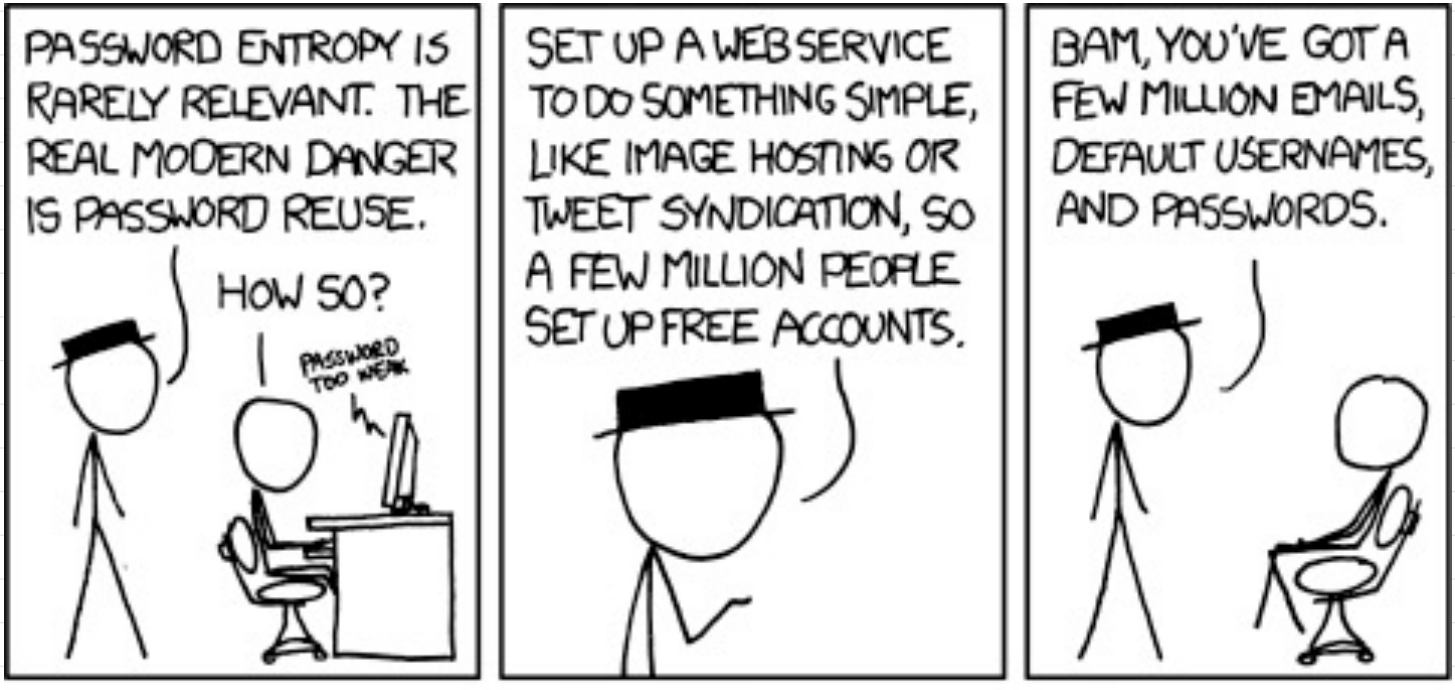
mathlife

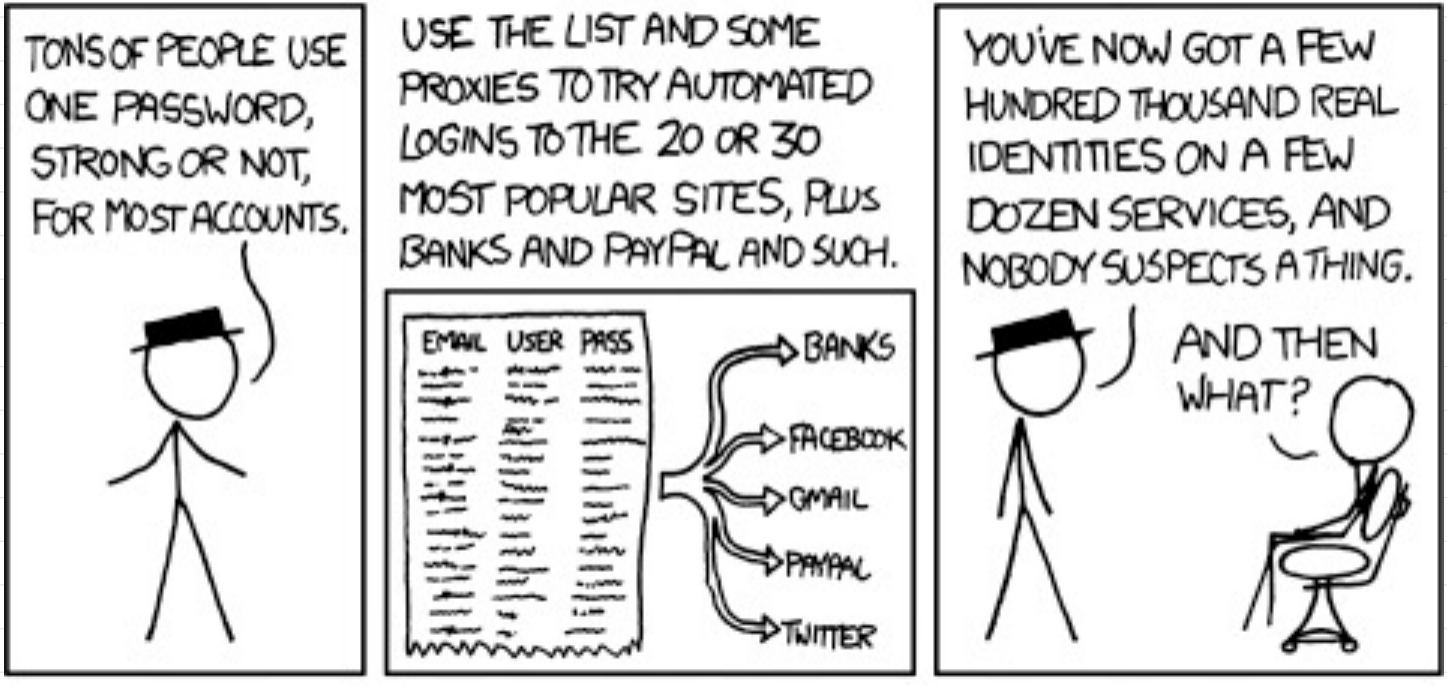
Change this password so that:

- It contains at least one number
- It contains at least one symbol (!, @, #, $...)
- It contains both lower case and upper case letters

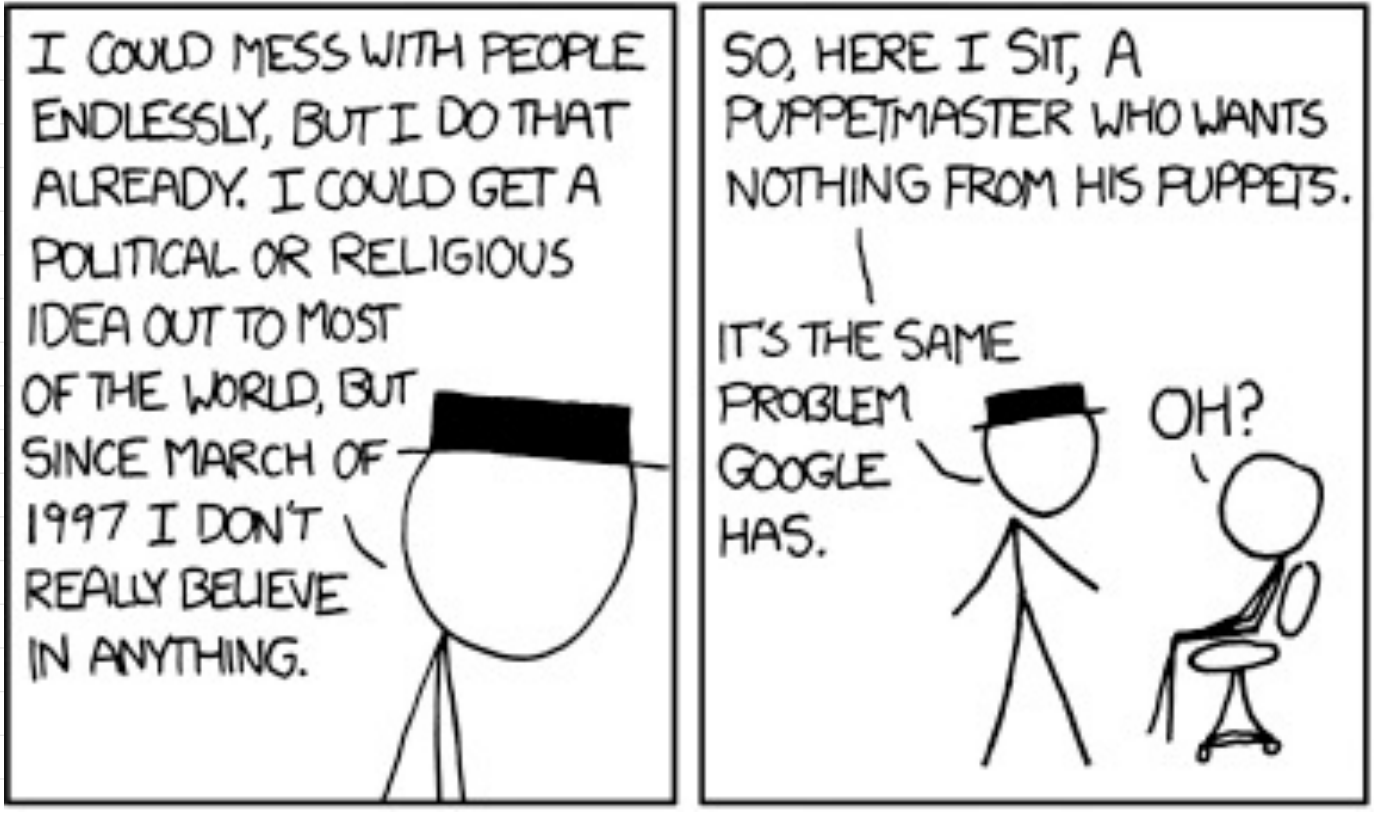
Even if a password looks complicated, it isn't necessarily good.

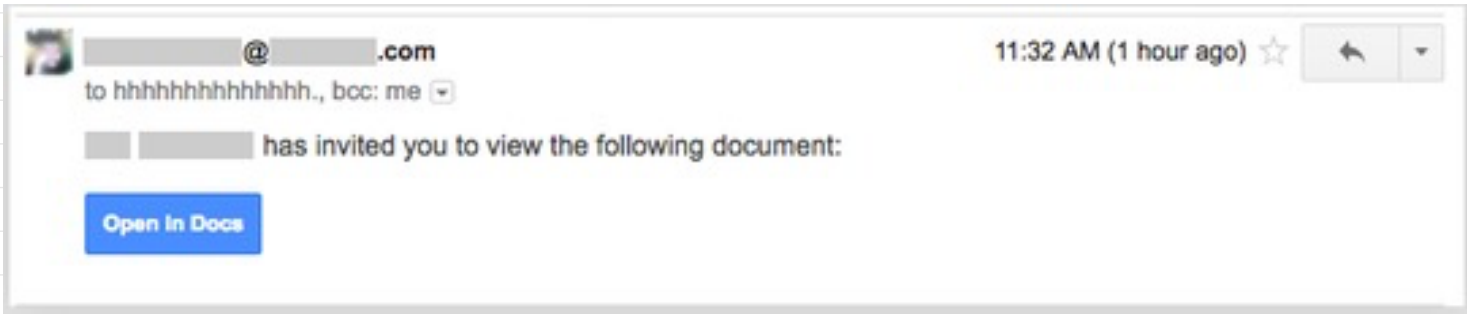
Some substitutions are very predictable.


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.


TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.
USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.
EMAIL
USER
PASS
BANKS
FACEBOOK
GMAIL
PAYPAL
TWITTER
YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.
AND THEN WHAT?


WELL, THAT'S WHERE I GOT STUCK.
YOU DID THIS?
WHY DID YOU *THINK* I HOSTED SO MANY UNPROFITABLE WEB SERVICES?
I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS CAREFULLY. BUT RESEARCH SHOWS MORE MONEY DOESN'T MAKE PEOPLE HAPPIER, ONCE THEY MAKE ENOUGH TO AVOID DAY-TO-DAY FINANCIAL STRESS.


I COULD MESS WITH PEOPLE ENDLESSLY, BUT I DO THAT ALREADY. I COULD GET A POLITICAL OR RELIGIOUS IDEA OUT TO MOST OF THE WORLD, BUT SINCE MARCH OF 1997 I DON'T REALLY BELIEVE IN ANYTHING.
SO, HERE I SIT, A PUPPETMASTER WHO WANTS NOTHING FROM HIS PUPPETS.
IT'S THE SAME PROBLEM GOOGLE HAS.
OH?


@ .com
11:32 AM (1 hour ago)
to hhhhhhhhhhhhhh., bcc: me
has invited you to view the following document:
Open in Docs

nytimes

The Most Important Step for Password Security

The Most Important Step for Password Security

don't tell people your password!

So... how do cryptographic hash functions work?

Ex MD5 is an example of a cryptographic hash function

- Designed by Ronald Rivest in 1991
- no longer considered secure
- collision found in 2005
- In 2009, a theoretical preimage attack was published

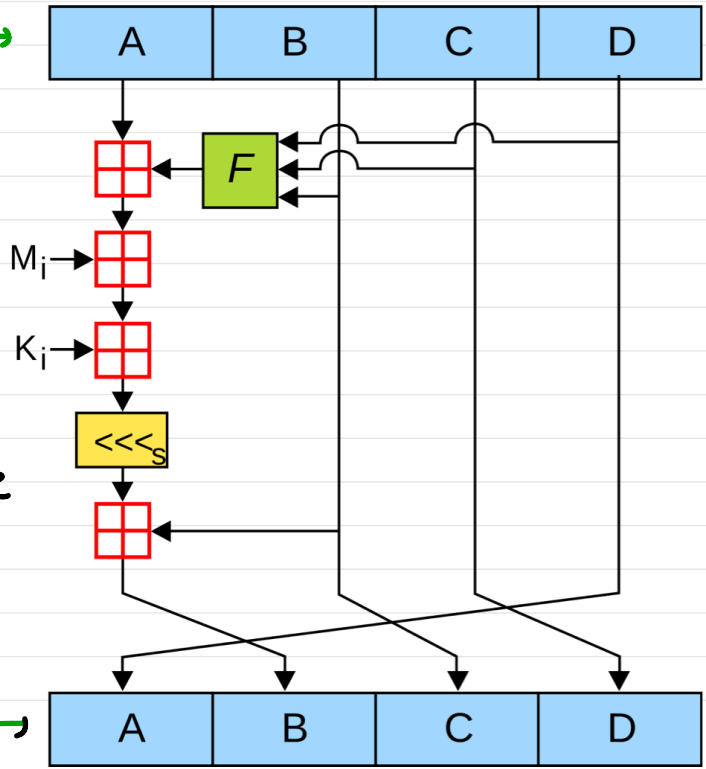
MD5

- Hash values are 128 bits (32 characters)
- Input is processed in blocks of length 512 bits (128 characters), padded if necessary.
- How the MD5 algorithm works is determined by its 128 bit state.
  - As we process the message, the message affects the state.
  - This means that what MD5 does is highly dependendent on the message
  - This is how we ensure that small changes to input cause large changes in the output.

One MD5 operation

- MD5 performs 64 of these (grouped in four rounds)

state at the beginning of the operation →



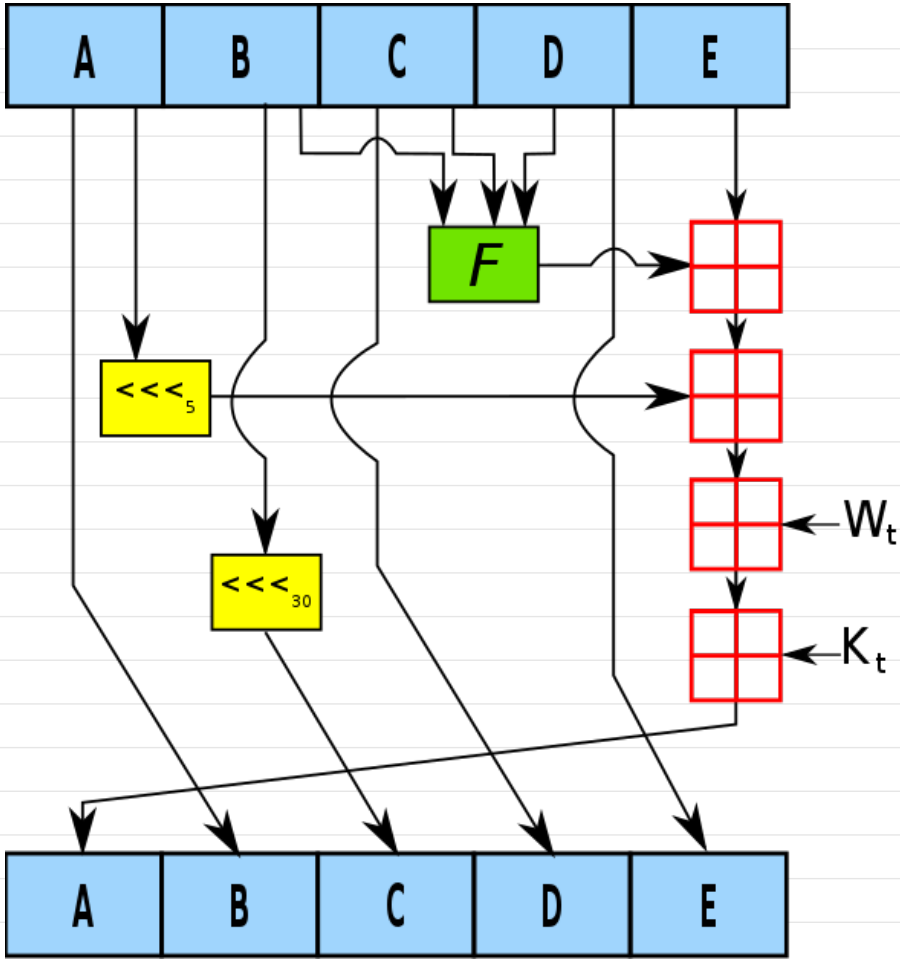
- There are four different functions F used (one for each round)
- ⊞ is addition mod 2^{32}
- $<<<_s$ is left circular shift by s digits (varies)
- M_i is part of the message
- K_i is a constant (varies)

state at the end of the operation →

Wikipedia

SHA-1

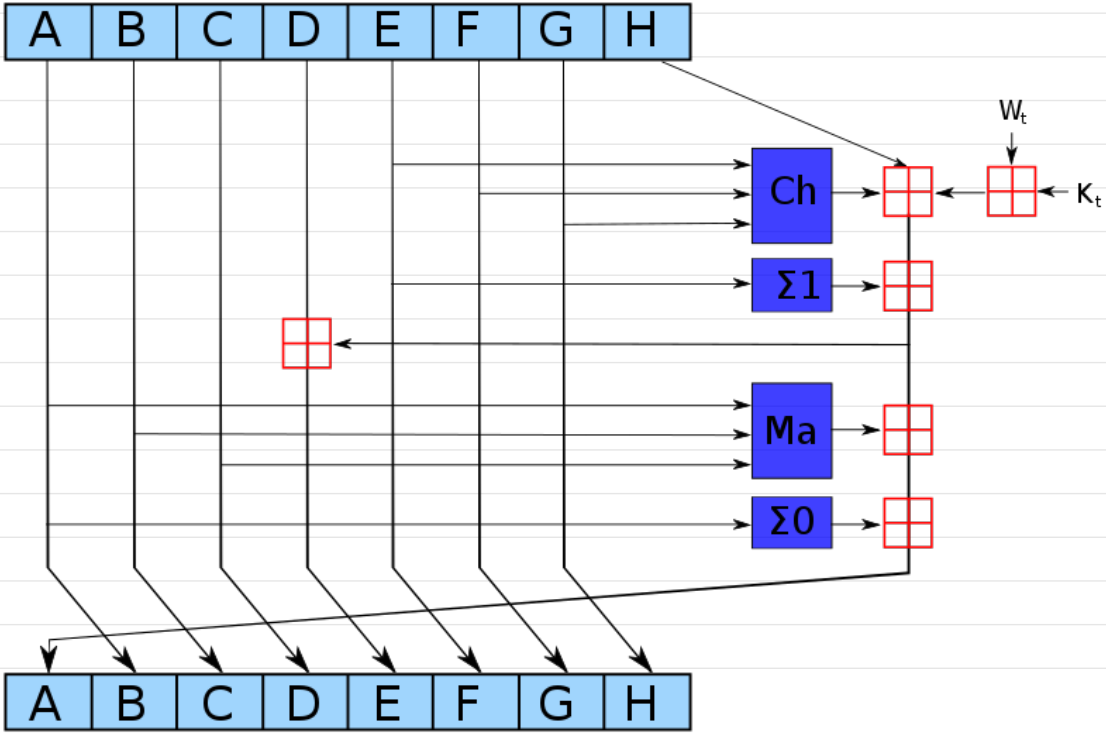
- designed by NSA
- no longer considered secure
- 2005 attacks found
- 2017 collision published



wikipedia

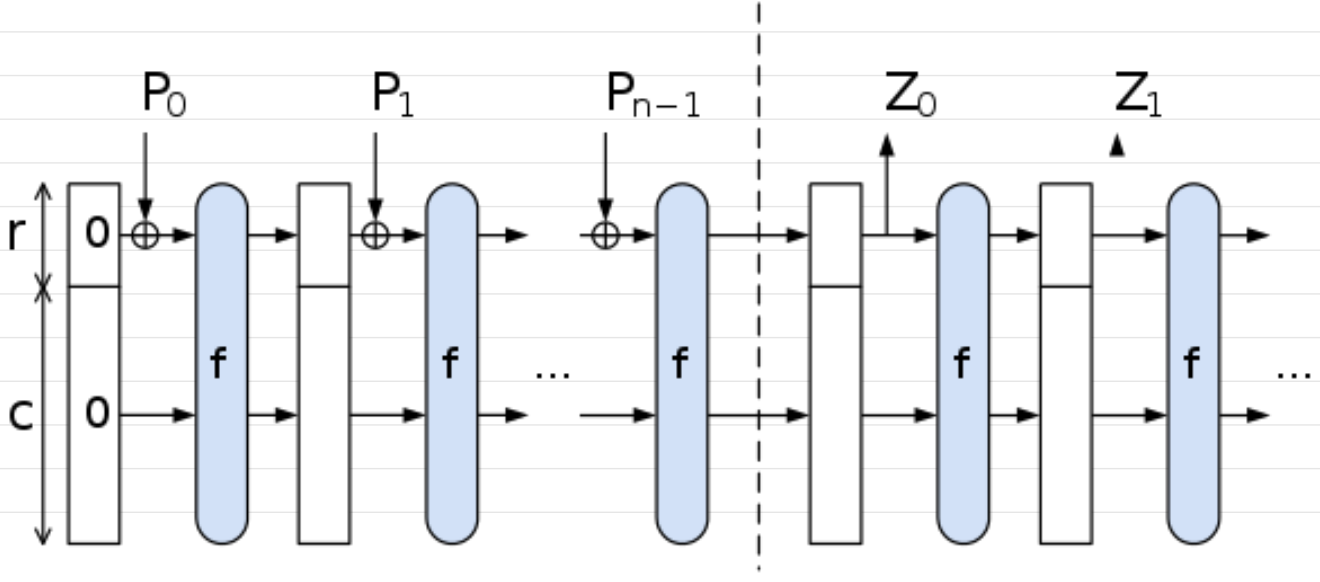
SHA-2

- published 2001 by NSA



SHA-3

- winner of NIST hash function competition in 2012, released in 2015.



Other applications:

- file verification – check if a file has been altered (intentionally or unintentionally)

  Ex When you download a file

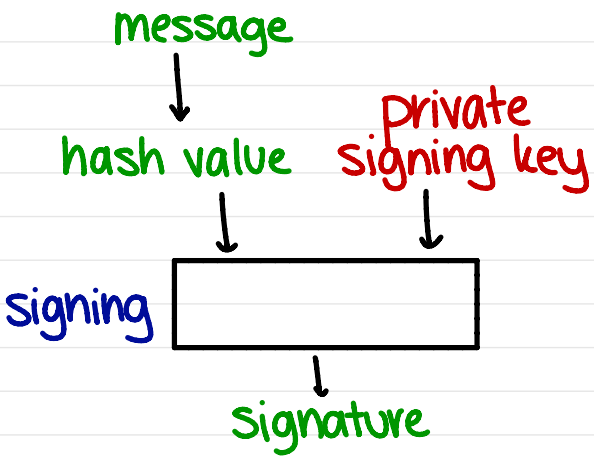
- digital signatures - verify authenticity of a document.

- bitcoin (and other cryptocurrencies)

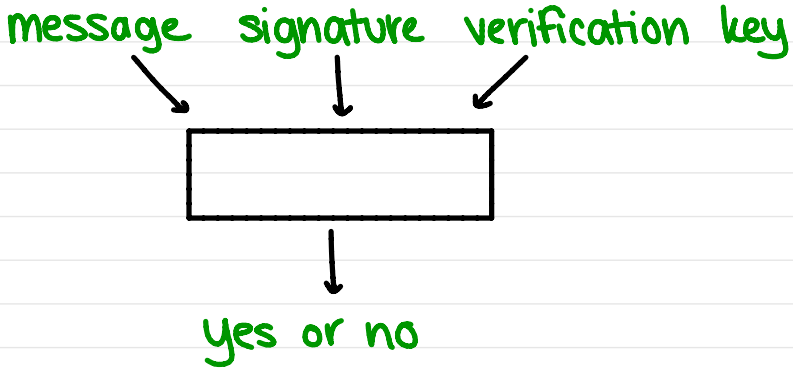
  - proof-of-work for generating bitcoin
  - signature to verify transactions
  - maintaining blockchain

Digital Signatures

Signing a message



Verifying a message



publish: message, signature, verification key

Final Question

Can you come up with a password system, so you have easy to remember, secure passwords that are different for different sites?