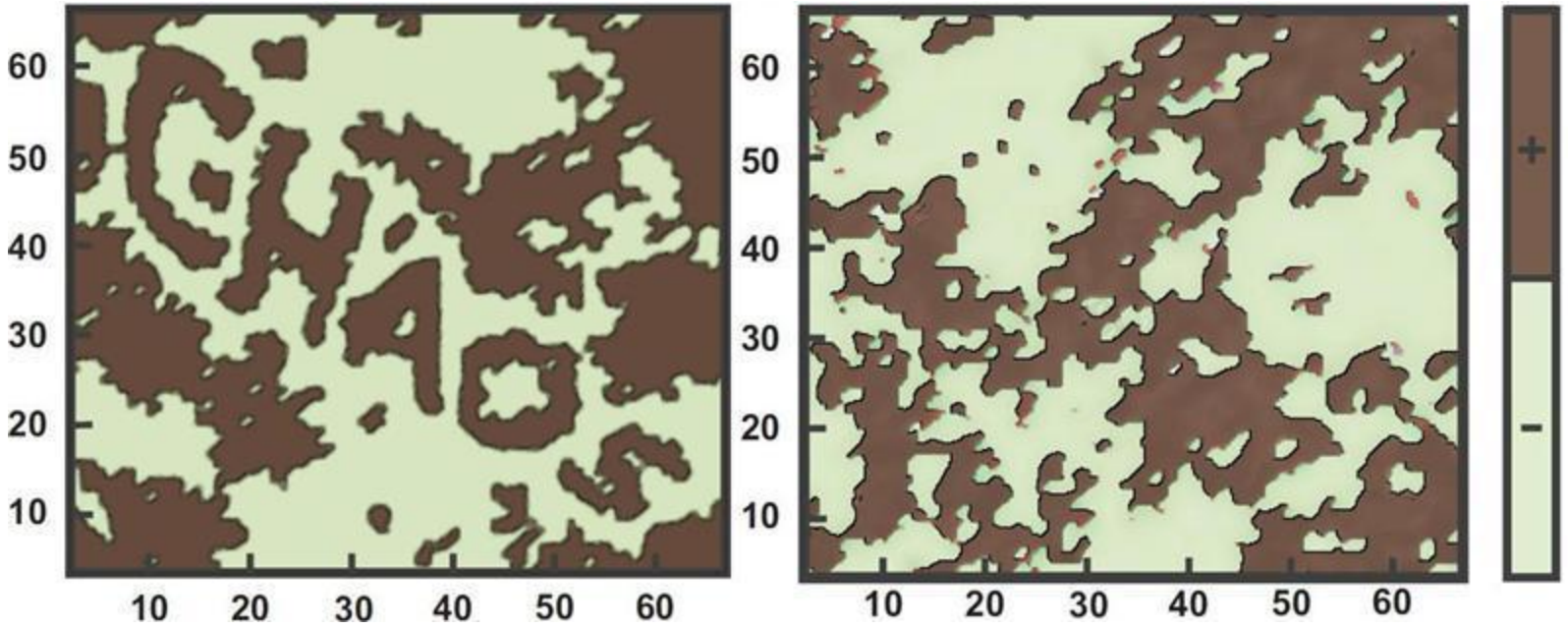

60
50
40
30
20
10
10 20 30 40 50 60
+
-


password

What means weak password?

passwords for: accounts, online services, credit/banking cards, ...

Test it:	Typical answer:
• how many passwords do you keep?	2-3...oh wait: 5-6...hm...15-20?
• how random and how long are they?	Not random, short
• are some of them equal or similar?	Sure, of course
• where do you keep or store them?	On a piece of paper, Post-it notes Files (not encrypted) ...

Diagnose: you have a problem with weak passwords

The weak password problem: chaos, criticality, and encrypted p-CAPTCHAs

S. Flach, MPIPKS Dresden

work done jointly with T. Laptyeva and K. Kladko: **arXiv:1103.6219**

- goal and basic idea
- what is the problem?
- a bit on encrypting and hacking
- and what are CAPTCHAs ?
- implementation of basic idea
- instead of conclusions: reactions from a virtual world

goal:

develop a scheme which allows you to

- memorize a short weak password
- have protection of a long strong password

basic idea:

- split a long strong password into two parts:
  short password SP + strong key SK
- memorize SP only
- encrypt SK with SP using CAPTCHA and phase transition

What is the problem with weak passwords?

- your data are hacked, stolen, destroyed
- companies make losses on identity fraud
  (total annual cost 2006 in US about $55 billion)

Consequence:

You are forced to memorize passwords which are:

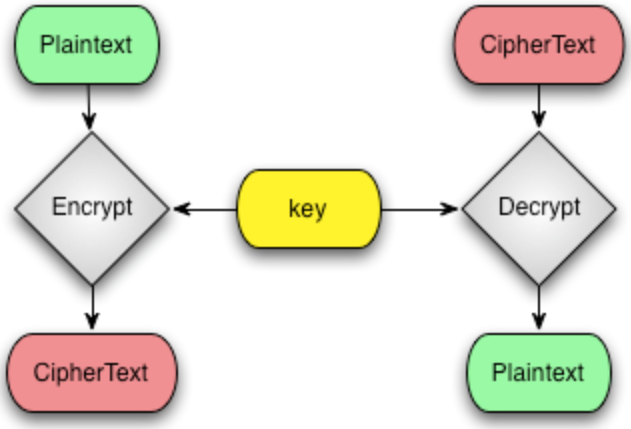
- **unguessable**
- **all different**
- **never written down**

These requests become unreasonable and unmanagable

A bit on data encrypting and hacking

Symmetric data encryption:

One password
Plaintext is correlated
Cipher Text is random-like

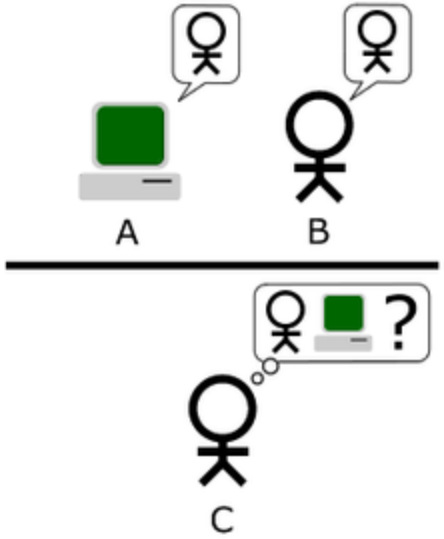


Hacking:

- **the hacker has all information except the password**
- **brute force method tries all passwords**
- **looks for correlations in decrypted candidate files**

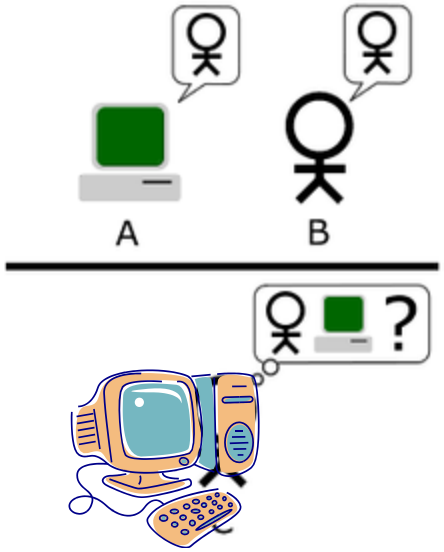
And what are CAPTCHAs?

Alan  **test:**



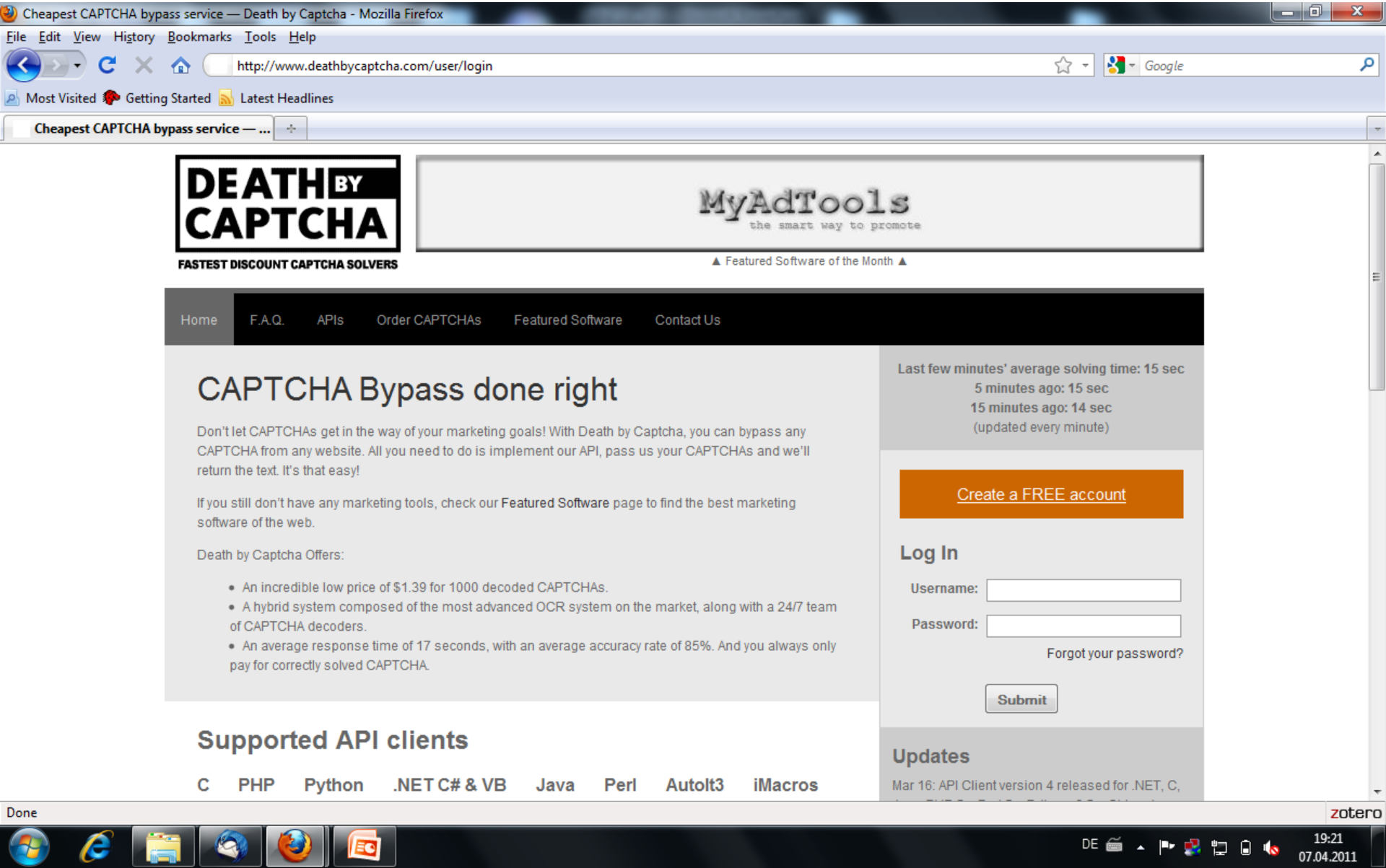
And what are CAPTCHAs?

CAPTCHA:



Completely Automated Public Turing test to tell Computers and Humans Apart

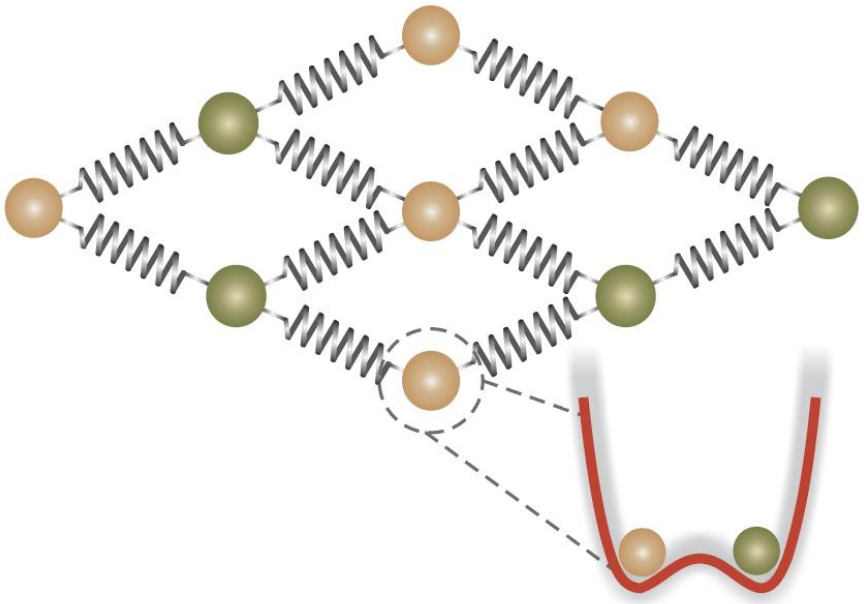
It takes about 1-10 seconds to perform a computer based CAPTCHA recognition



Implementation of basic idea

$$\mathcal{H} = \sum_{i,j=1}^{N} \left(\frac{1}{2} p_{ij}^2 - \frac{1}{2} u_{ij}^2 + \frac{1}{4} u_{ij}^4 + \mathcal{F}_{ij} \right)$$

$$\mathcal{F}_{ij} = \sum_{k=\pm 1} \frac{1}{2} \left[(u_{i+k,j} - u_{ij})^2 + (u_{i,j+k} - u_{ij})^2 \right]$$

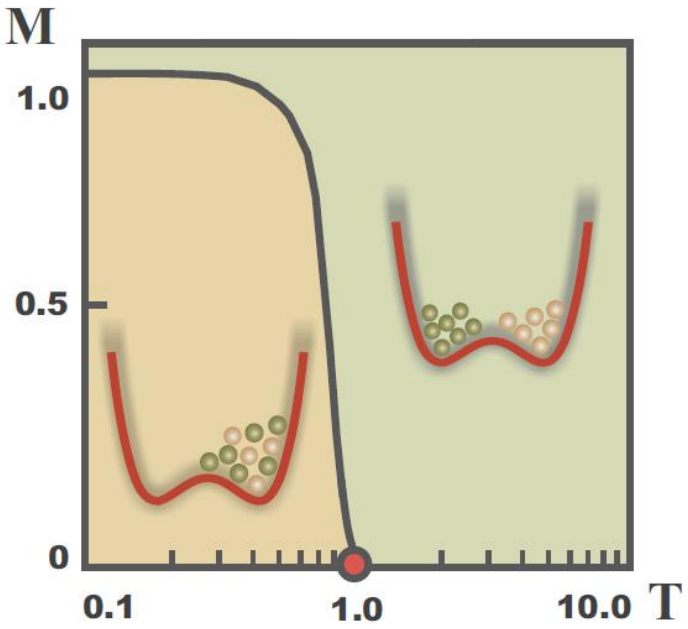


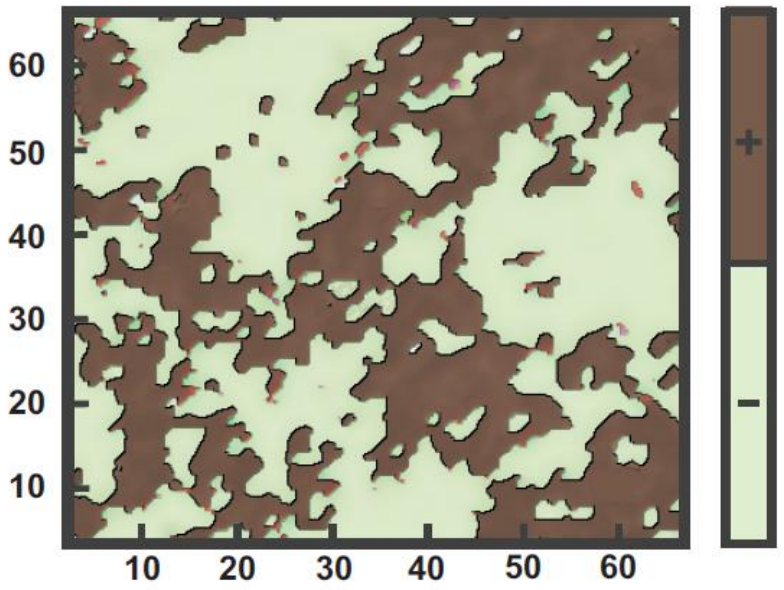
Phase transition

order parameter $M = \frac{1}{N^2} \left| \sum_{ij} \mathrm{sign}(u_{ij}) \right|$

temperature: here simply energy density

opertional point: close to transition



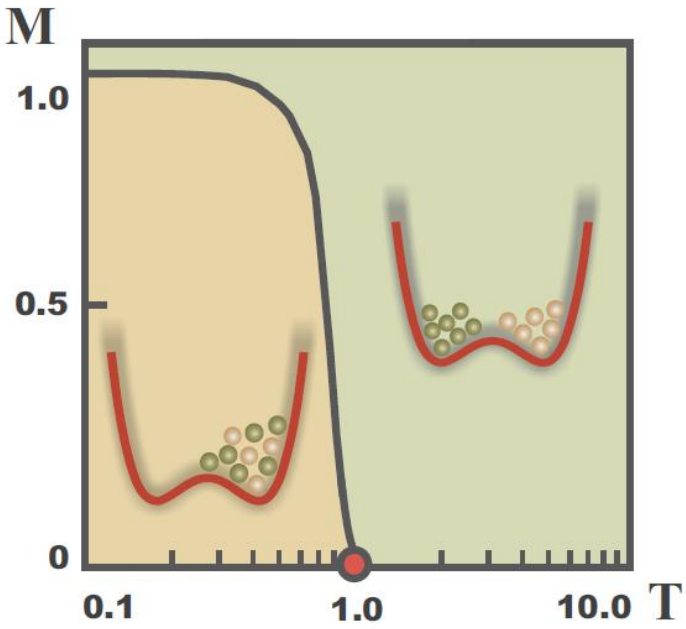


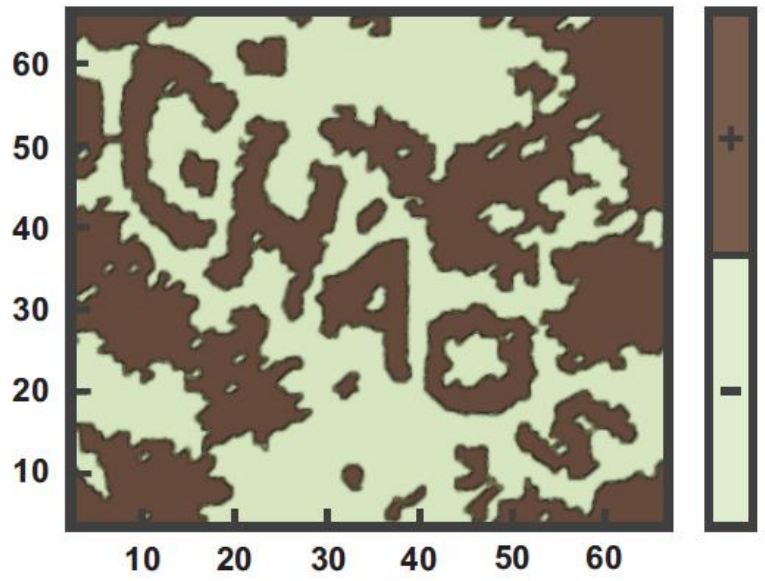
Phase transition

order parameter $M = \frac{1}{N^2} \left| \sum_{ij} \mathrm{sign}(u_{ij}) \right|$

temperature: here simply energy density

opertional point: close to transition

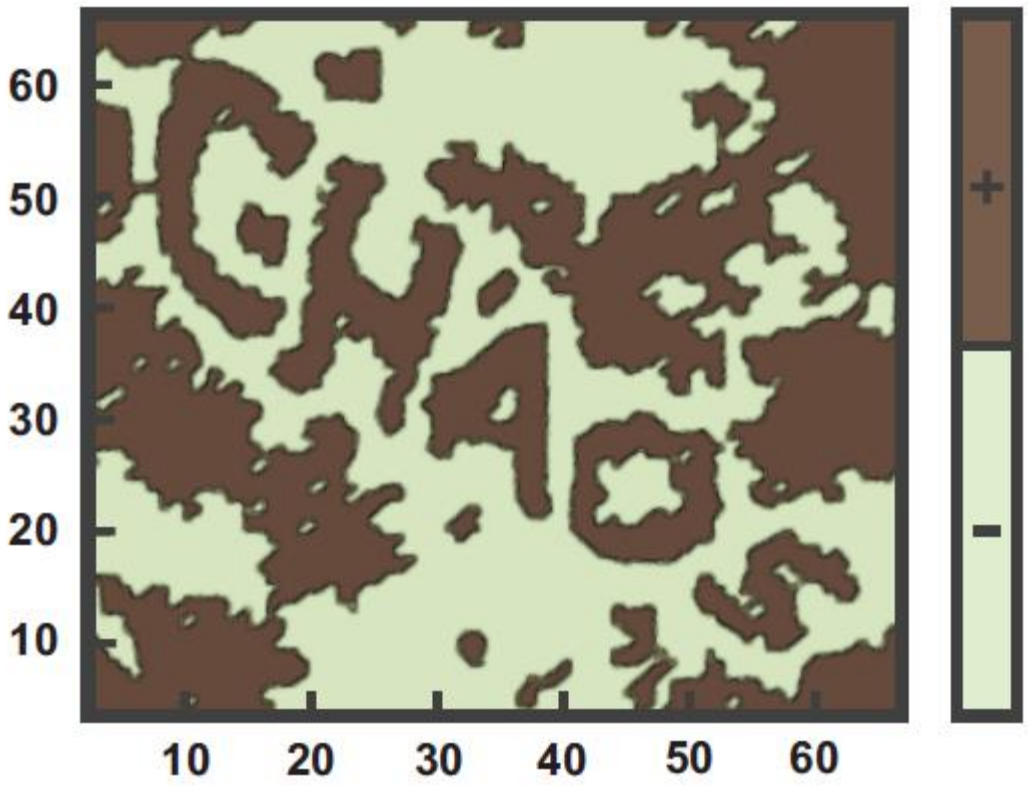




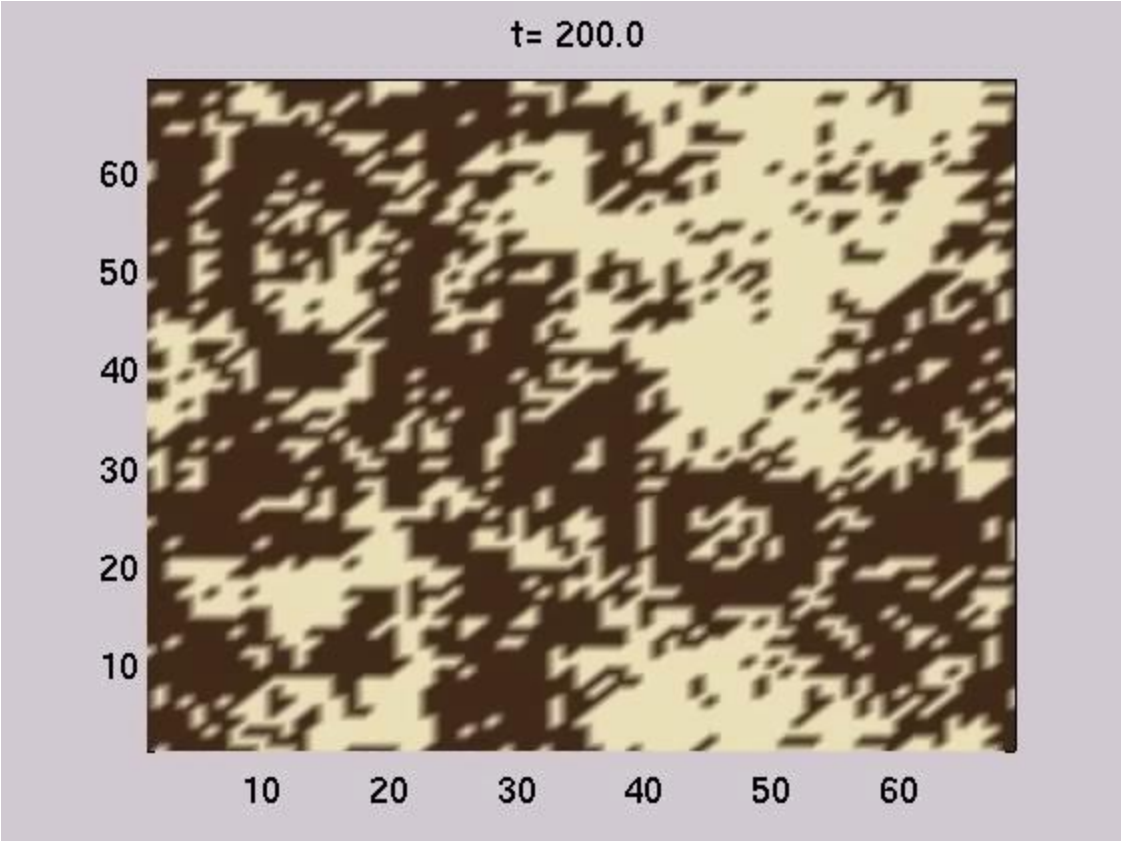
Maximum return time and chaos

- consider an initial state image at time t=200
- define a suitable error function for blurring images
- use symplectic time reversible integrator (Verlet or leap-frog)
- stop at time t=T and return to t=200
- due to roundoff errors and chaos we do not return exactly
- measure blurring
- measure maximum Tm up to which recovering is possible
- measure largest Lyapunov coefficient: proportional to Tm

Imprint the strong key SK

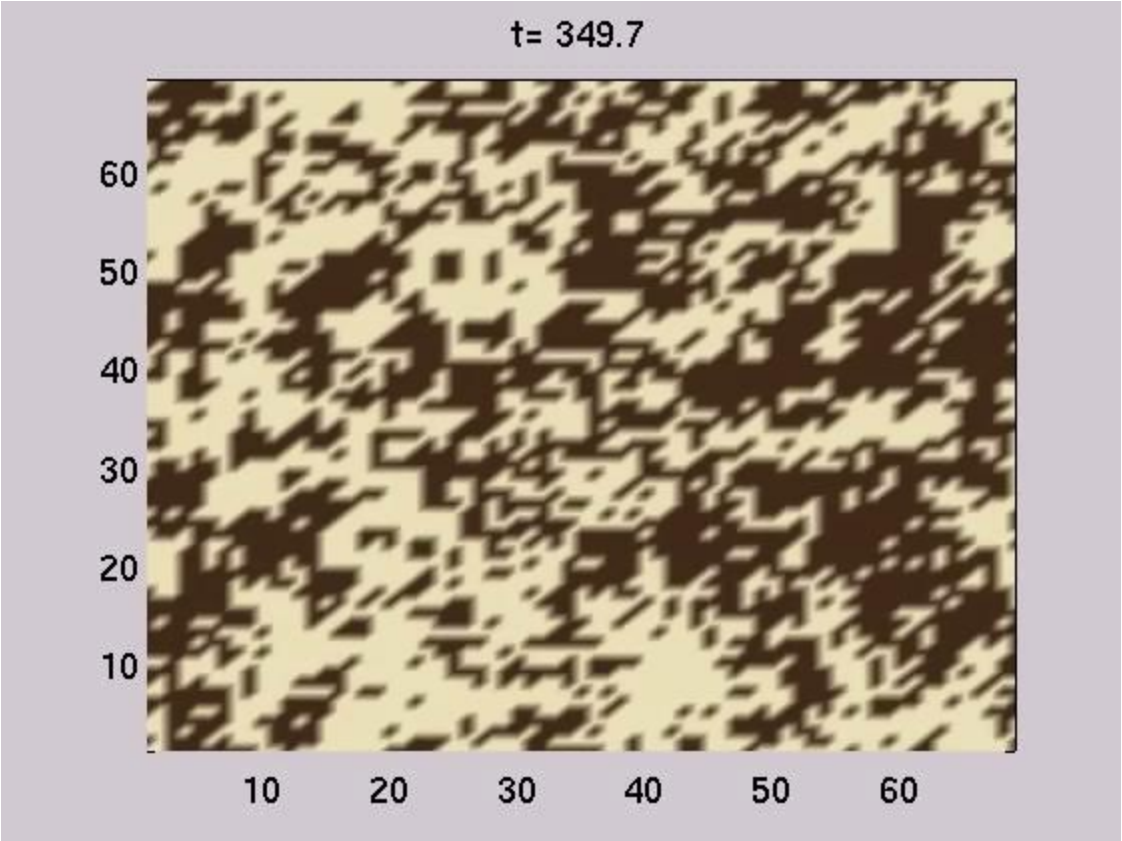


Evolve forward in time up to the edge of chaos



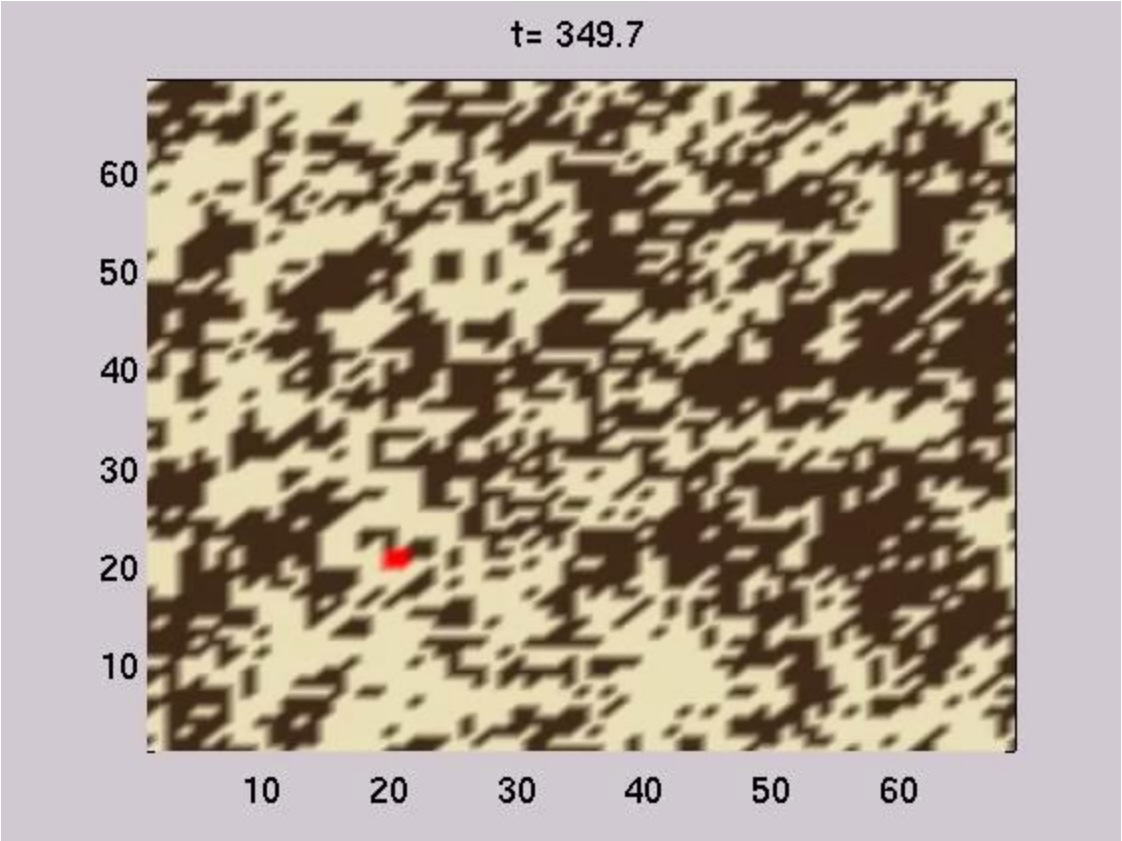
Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!

Can we return back?

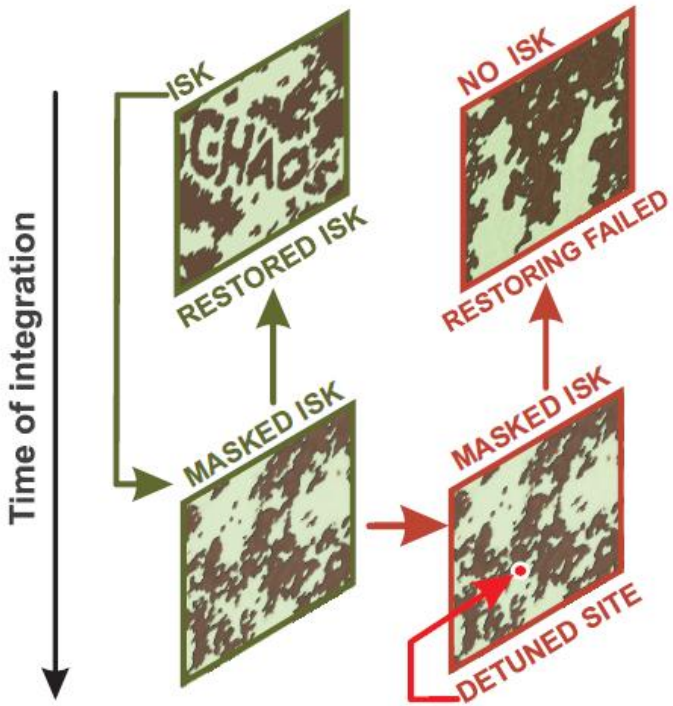


Decrypt F2 using short password
Glue F1 and F2 together to obtain the correct final dynamical state
Integrate backwards in time
Read the strong key SK!

Detune one oscillator coordinate by 0.000001



The scheme in a nutshell



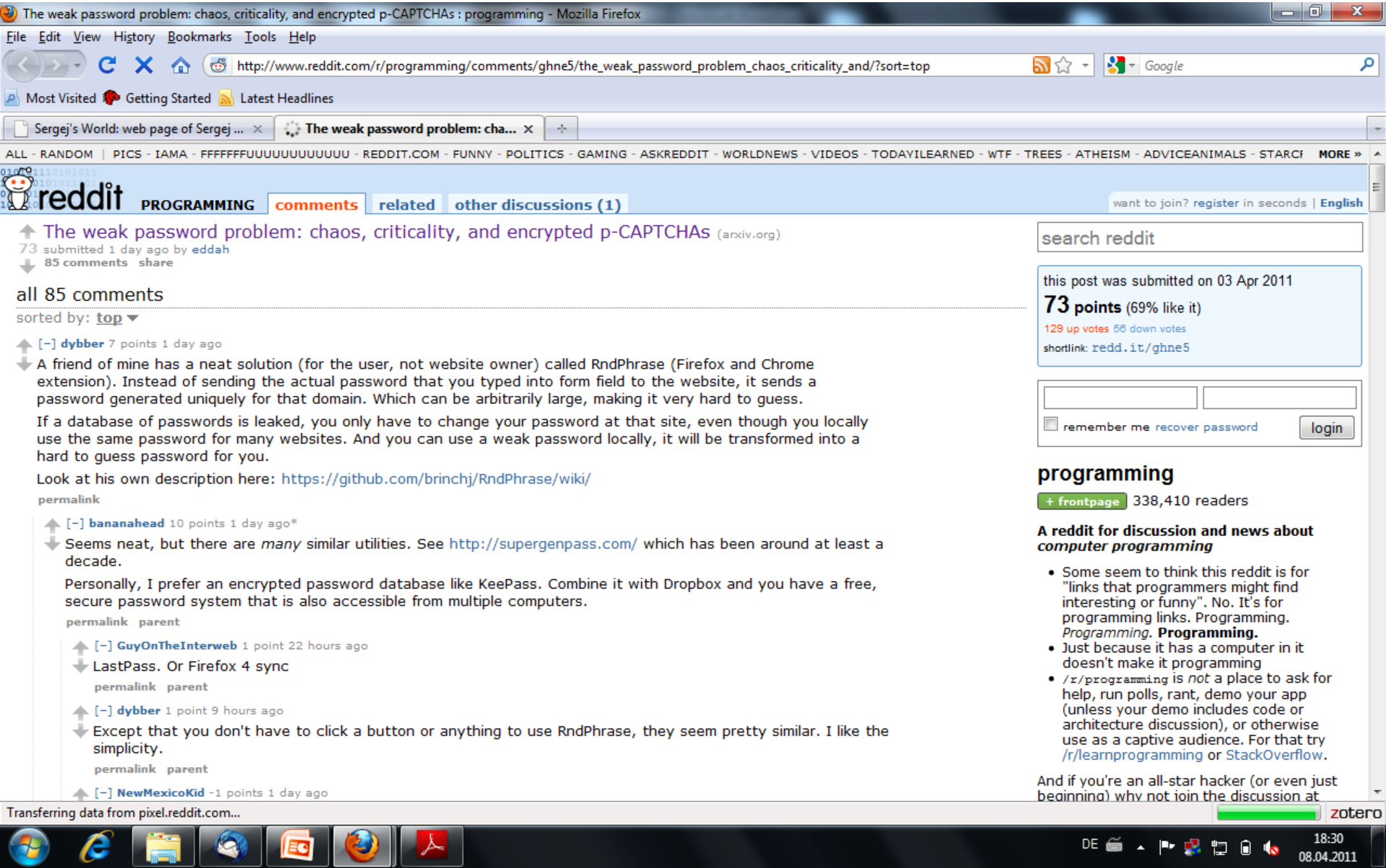
Store the final state (coordinates, momenta) in two files:
F1 contains signs and all significant digits
F2 contains the rest
Encrypt F2 using short password!

Fast hacking of strong key impossible:

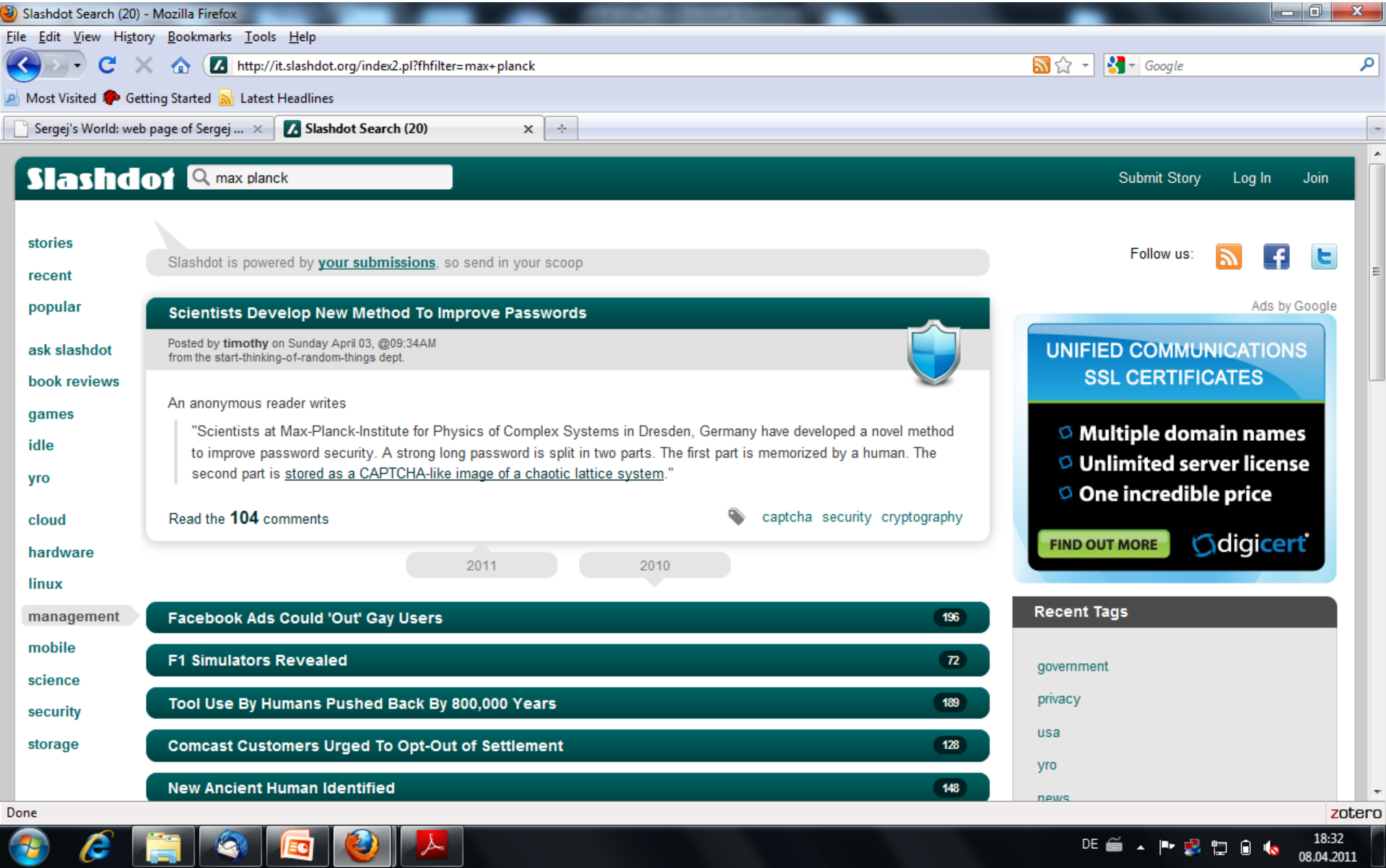
- **via correlations – they are always large**
- **CAPTCHA recognition – too long even with SP**

Reactions of a virtual world

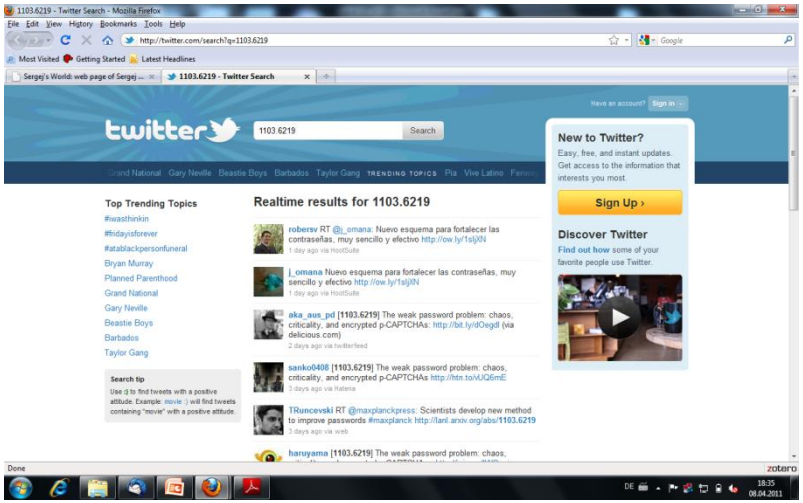
Reactions of a virtual world

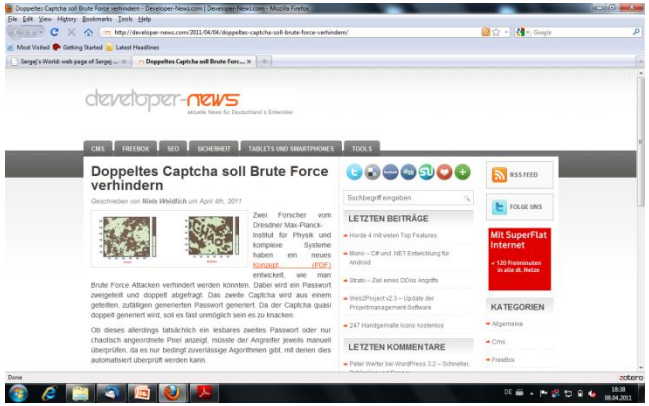


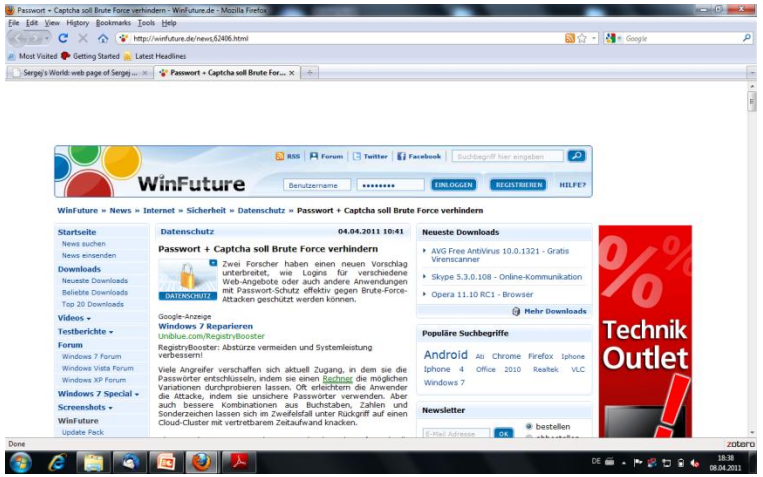
Reactions of a virtual world

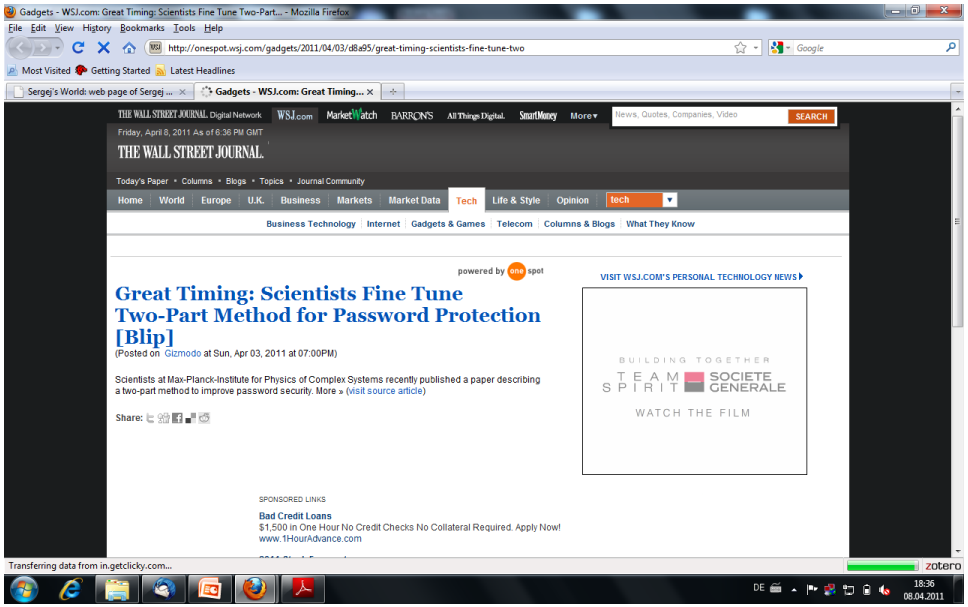


Reactions of a virtual world

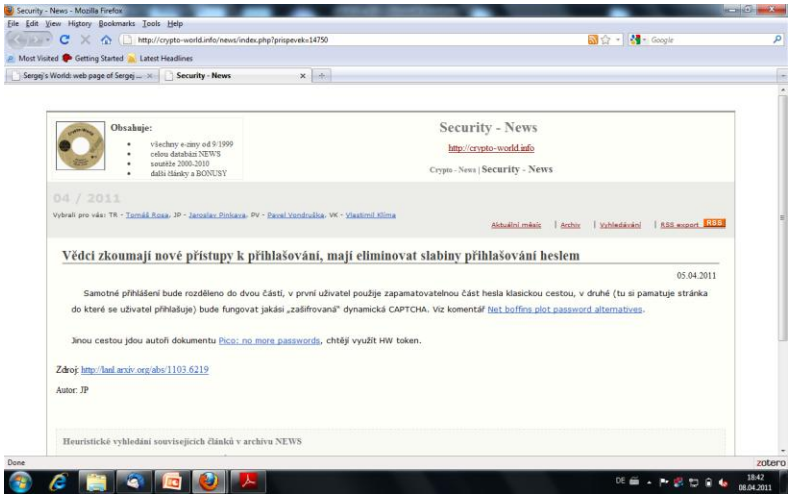


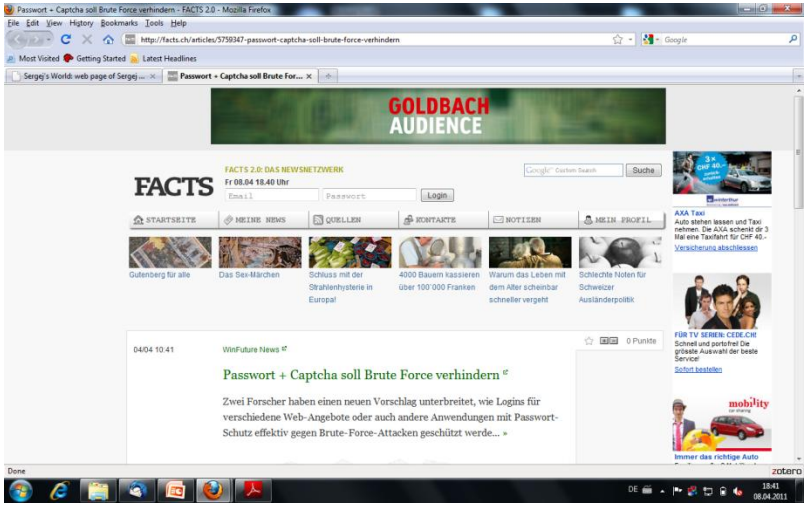






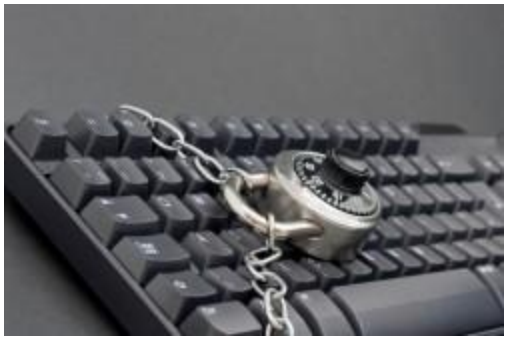
Reactions of a virtual world





Reactions of a virtual world

Featured on more than 180 web sites including rambler.ru , mail.ru, yandex.ru etc



Pikachu - Wikipedia, the free encyclopedia - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://en.wikipedia.org/wiki/Pikachu

Most Visited Getting Started Latest Headlines

Pikachu - Wikipedia, the free encyclo...

Log in / create account

WIKIPEDIA
The Free Encyclopedia

Article Discussion Read View source View history Search

Pikachu

From Wikipedia, the free encyclopedia

Not to be confused with Picacho or Pika.

Pikachu (ピカチュウ *Pikachū*?) is one of the species of Pokémon creatures from the *Pokémon* media franchise—a collection of video games, anime, manga, books, trading cards, and other media created by Satoshi Tajiri. As do all Pokémon, Pikachu fight other Pokémon in battles central to the anime, manga, and games of the series.[1] Pikachu is among the most recognizable Pokémon, largely because a Pikachu is a central character in the *Pokémon* anime series. Pikachu is widely considered the most popular Pokémon,[2] is regarded as the official mascot of the Pokémon franchise, and has become an icon of Japanese culture in recent years.

Within the world of the Pokémon franchise, Pikachu are often found in houses, forests,[3] plains, and occasionally near mountains, islands, and electrical sources (such as power plants), on most continents throughout the fictional world. As an Electric-type Pokémon, Pikachu can store electricity in its cheeks and release it in lightning-based attacks.[4]

Contents [hide]

1 Concept and creation

Pikachu

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact Wikipedia