

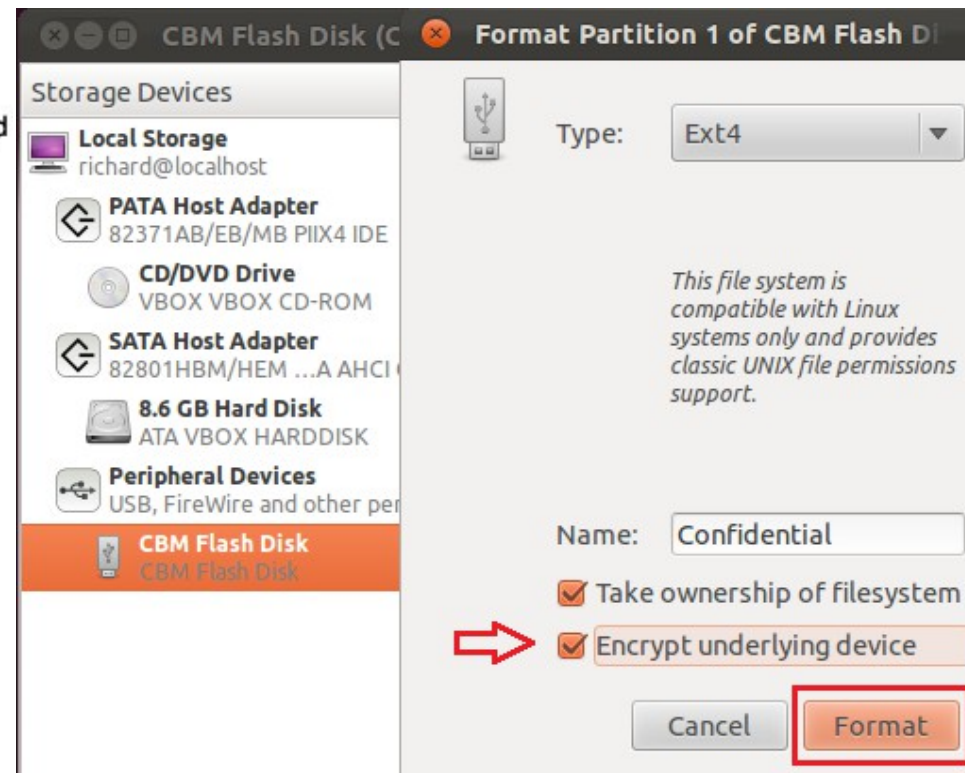
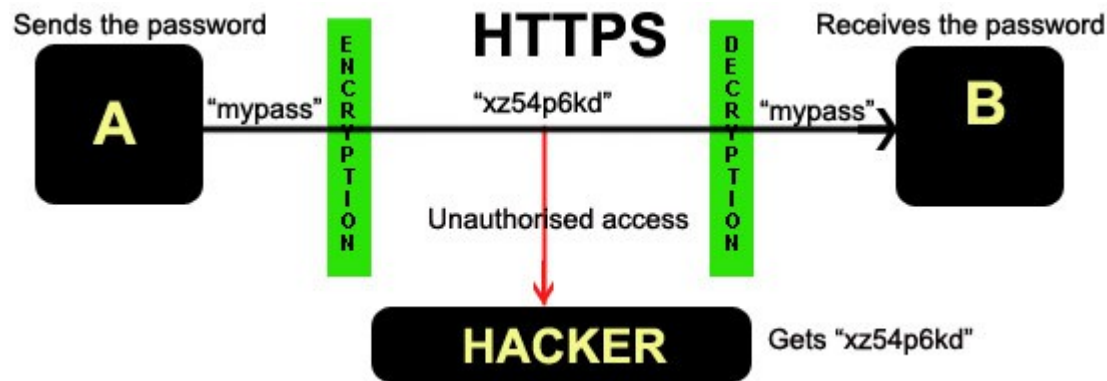
COMPUTER SECURITY

INTRODUCTION TO
CRYPTOGRAPHY

Willy Sudiarto Raharjo

Teknik Informatika
Universitas Kristen Duta Wacana

Cryptography is Everywhere



LinkedIn passwords in circulation – Update

Internet forums are currently circulating a list containing over six million password hashes which allegedly originate from [LinkedIn](#). The passwords are being cracked collaboratively with about 300,000 passwords already published as plaintext.



The list contains pure SHA1 hashes with no name or email addresses. If decrypted, the passwords will not easily give access to an appropriate account. However, it is probable that the person who captured the hashes also has the corresponding email addresses. In an initial sampling, **The H's** associates at heise Security didn't find any known LinkedIn passwords in the list, but with over 160 million members that doesn't mean a lot. The already cracked passwords often contain "linked" or even "linkedin" in the form, for example, of "lawrencelinkedin". This suggests that the passwords actually come from the LinkedIn social network. However, this has not yet been confirmed.

The shocking reality is that even passwords "parikh093760239", "a06v1203n08" and "376417miata?" have already been cracked. This is due to the fact that the hashes were obviously generated without salt. This makes them easy targets for attacks using rainbow tables, which makes it possible to crack even passwords that are believed to be strong in just a few hours. For a view of what a server administrator needs to do to prevent this, read the article [Storing passwords in uncrackable form](#) at **The H Security**.

8 June 2012, 10:45

« previous | next »

Millions of Last.fm passwords leaked

A list with several million passwords belonging to users of the music community site [Last.fm](#) has been posted on the internet. The site owners have posted [a statement](#) saying that the company is investigating the leak and that all users of the service should change their passwords immediately. This is the third major compromise of a popular web site's passwords in as many days.



The H's associates at heise Security are in possession of a list containing approximately 2.5 million password hashes. Like the recently leaked data from [eHarmony](#), these are unsalted MD5 hashes that are trivial to crack in today's world of fast CPU and GPU hardware and specialised techniques such as using [rainbow tables](#). At least one million of these hashes have already been cracked and the clear text passwords have also been posted on the internet. The hashes that were leaked from [LinkedIn](#) were generated using the SHA-1 algorithm.

450,000 email addresses and plain-text passwords in circulation

A list of over 450,000 email addresses and plain-text passwords, apparently from users of a Yahoo! service, is in circulation on the internet. [According to](#) security expert and former hacker Kevin Mitnick, the passwords belong to the little-known VoIP service, [Yahoo! Voice](#).



The information is contained in a 17MB text file and has been released by a group of hackers calling themselves the D33DS Company. Access to the original information is said to have been achieved through use of an SQL injection vulnerability, where databases are accessed through inadequately filtered parameters passing through the web front end.

Whether the passwords were originally stored as plain text in the database or if the hackers had already cracked hashed passwords to produce the file is unclear. The latter would mean that the 450,000 records are just those for which the hackers were able to identify the hashed passwords plain text equivalent, and that, in turn, would also mean that the actual extent of stolen data could be even higher. Yahoo! has yet to answer requests for comment.

7 June 2012, 12:55

« previous | next »

eHarmony admits to leaking 1.5 million passwords

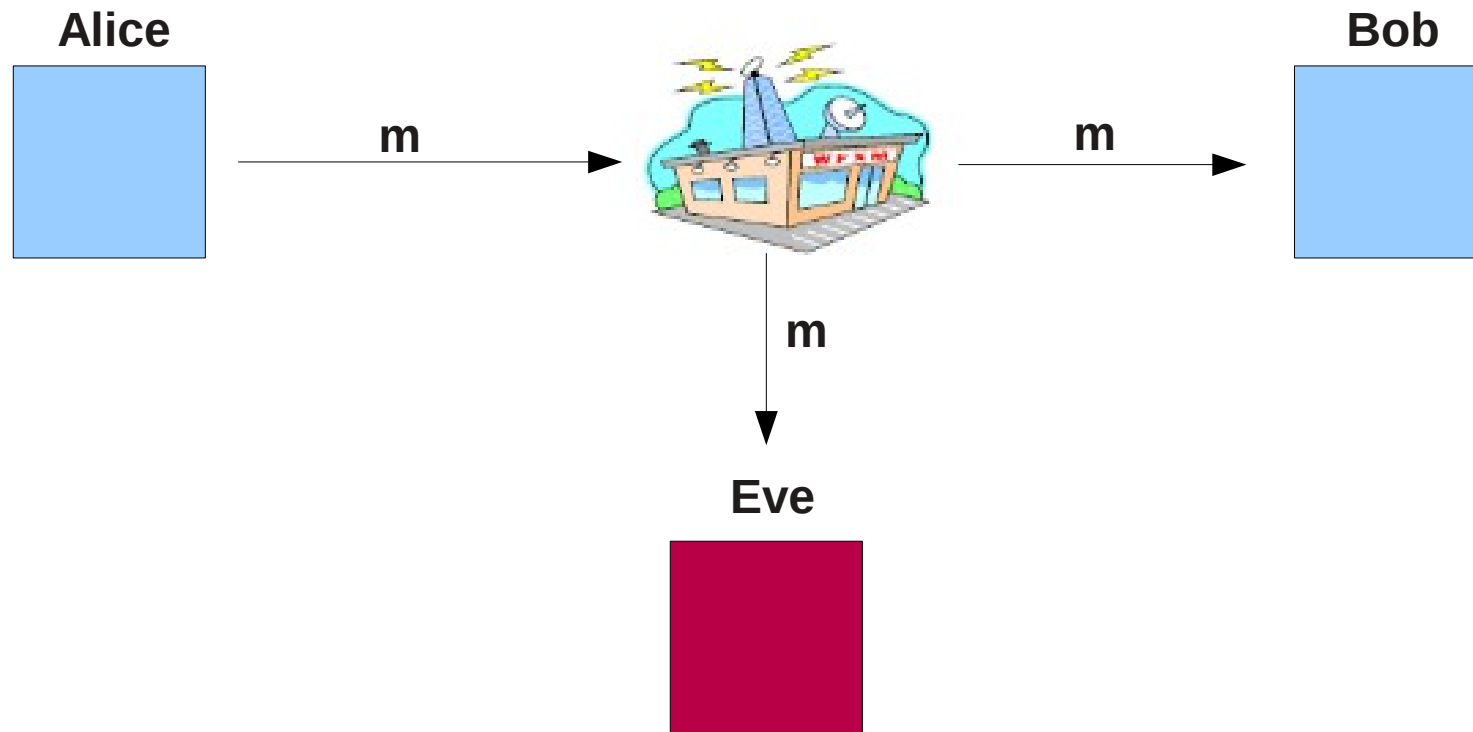
Dating site [eHarmony](#) has [admitted](#) that its password database has been compromised, with around 1.5 million hashed passwords being found in the wild. The leaked database that appeared in public contained unsalted MD5 hashed passwords and was reported to not contain any identifying usernames or email addresses.



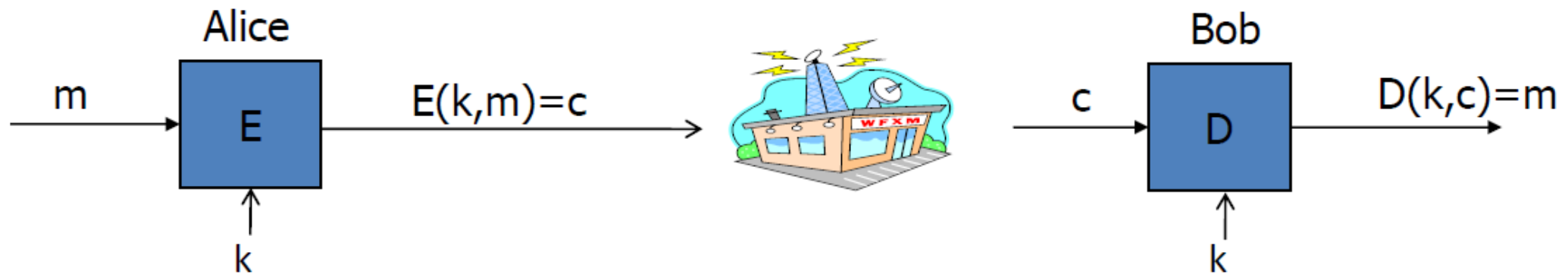
According to [reports](#), the password hashes were posted to a forum where a user asked for help in cracking the hashes. This help was collectively given by the forum members who were then reportedly given the LinkedIn hashed passwords to work on. It is possible that the person who provided the uncracked password list has a copy of the passwords complete with identifying information.

eHarmony described the 1.5 million passwords as a "small fraction" of its user base. As with LinkedIn's [admission](#), eHarmony gave no details of how the passwords were leaked and says it is continuing to investigate what happened. Unlike LinkedIn, it gave no assurances that it had or will be updating the way it stores passwords.

Common Scenario



Basic Concept of Encryption



E, D : cipher k : secret key (e.g. 128 bits)

m, c : plaintext, ciphertext

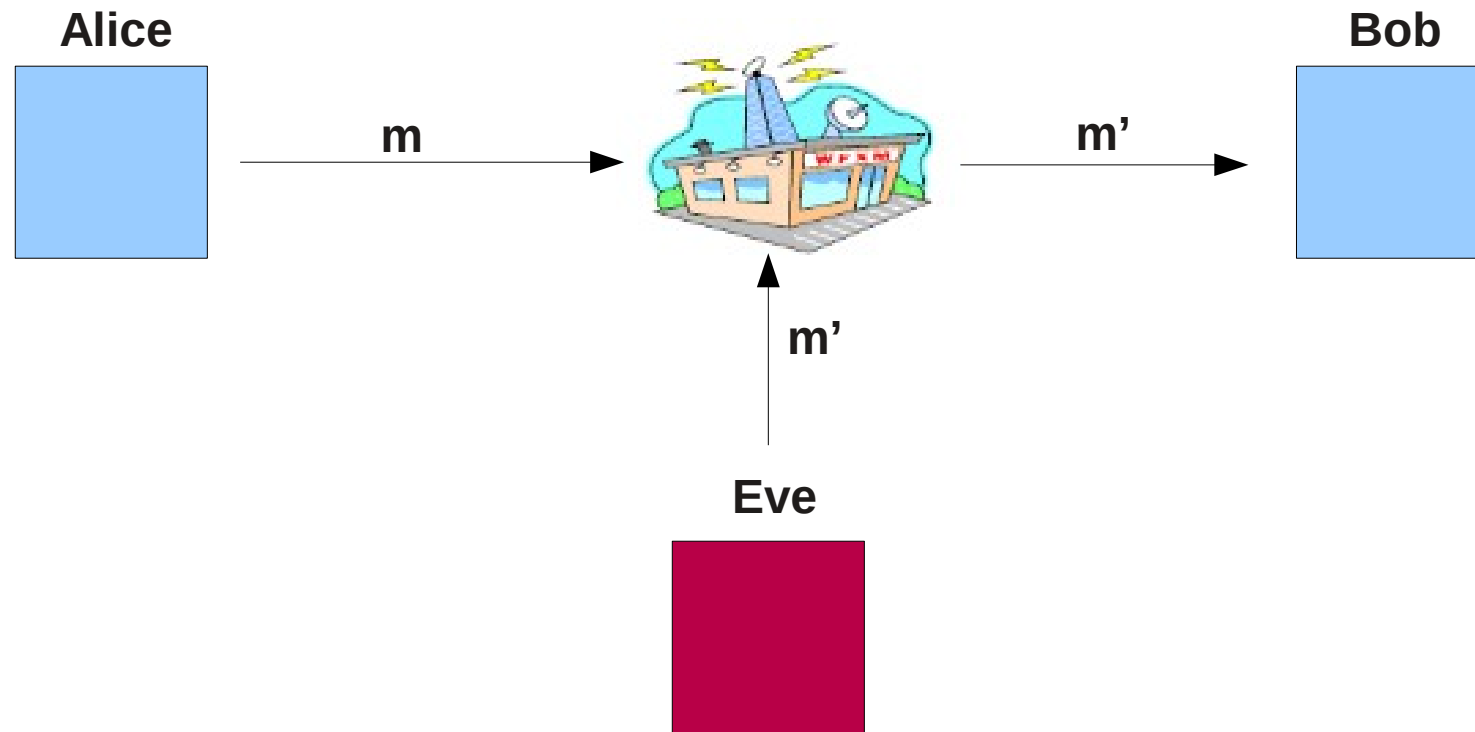
Encryption algorithm is **publicly known**

- Never use a proprietary cipher

Kerckhoffs' Principle

The security of the encryption scheme must depend only on the secrecy of the key K_e , and not on the secrecy of the algorithm

Common Scenario



How does Bob know who sent the message?

Authentication

“a” is called Message Authentication Code (MAC)

Alice

$$m, a := h(K_a, m)$$

m, a



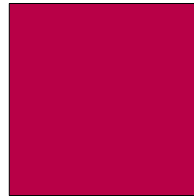
m, a

Bob

$$m, a := h(K_a, m)$$

m'

Eve



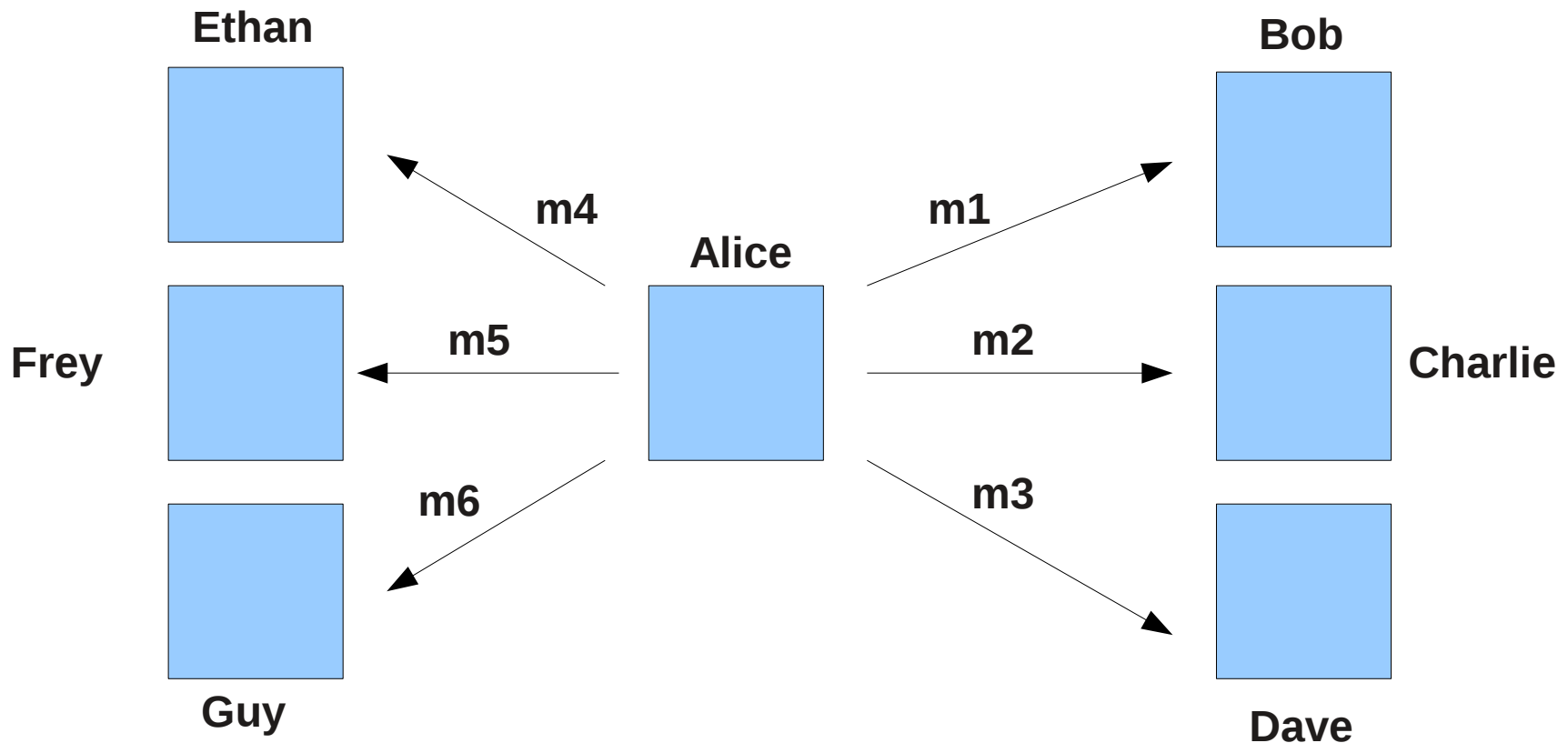
What if Eve use a replaying attack on Bob?

Encrypting a message doesn't stop people to
manipulate it's content

Authenticating a message doesn't keep the
message secret

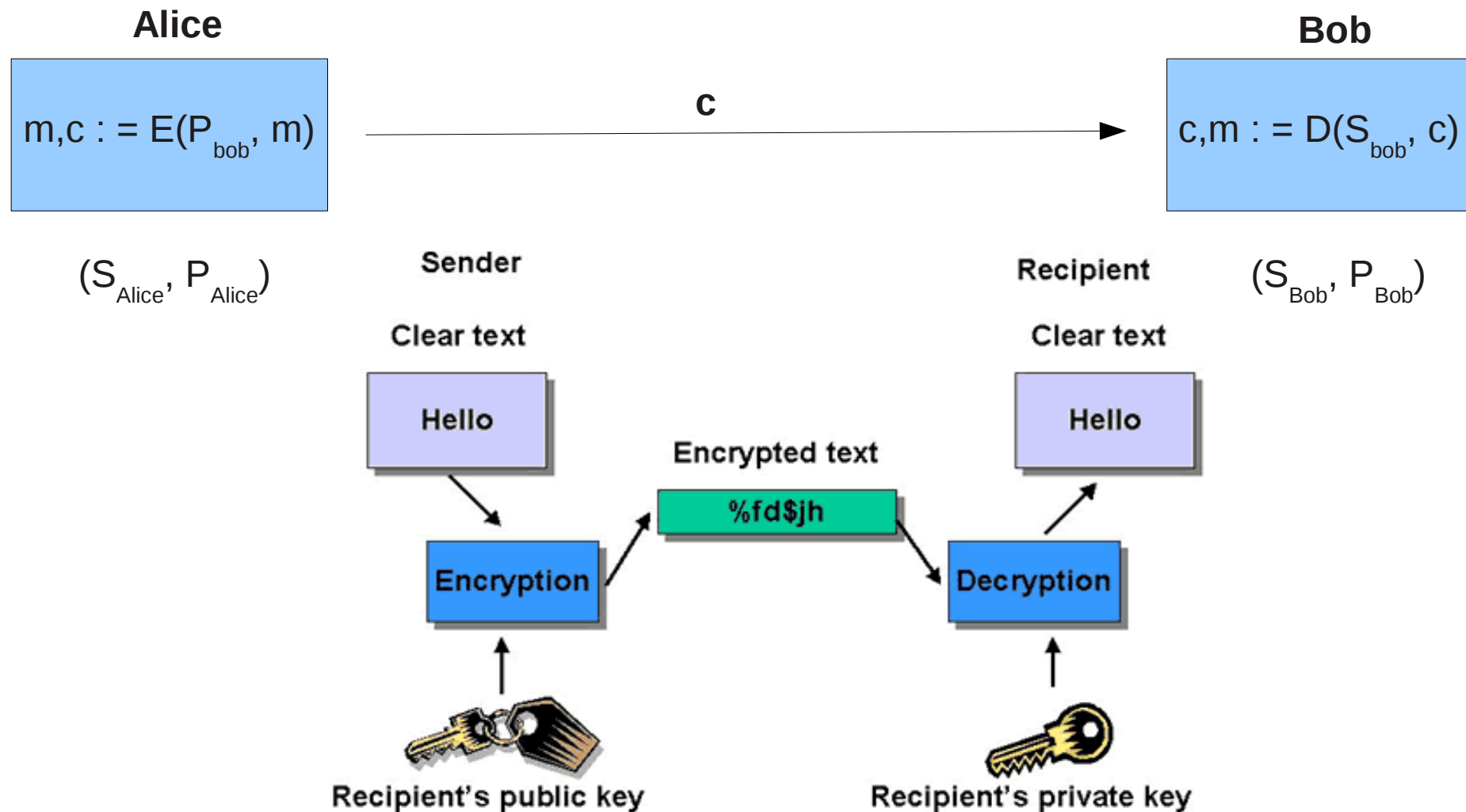
Cryptography relies on other technology to
be perfect

Common Scenario



How many keys should be created and maintained?

Public Key Cryptography



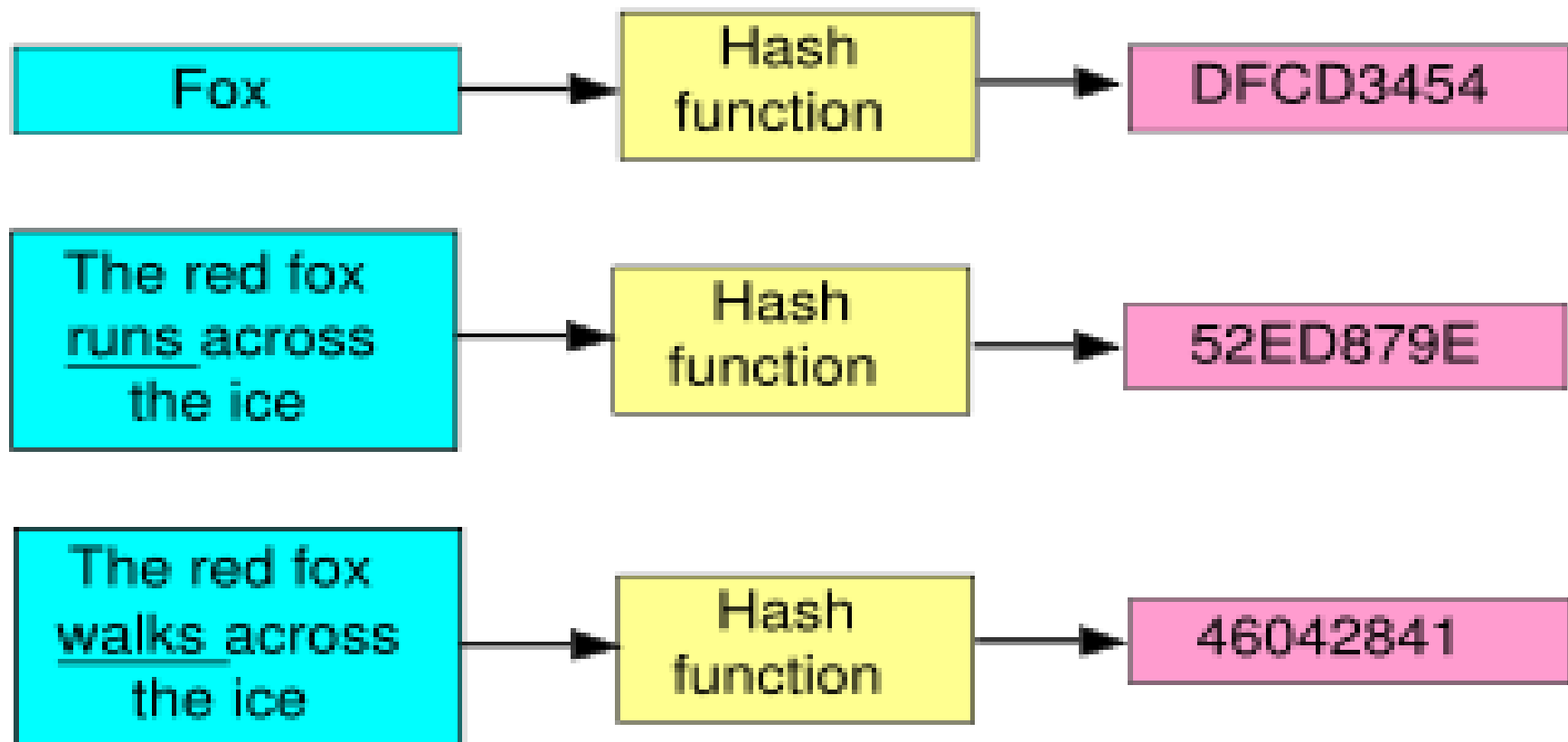
Trivia Quiz

If asymmetric cryptography can solve key management, why don't we all use public-key cryptography and leave symmetric key cryptography behind?

Hash Functions

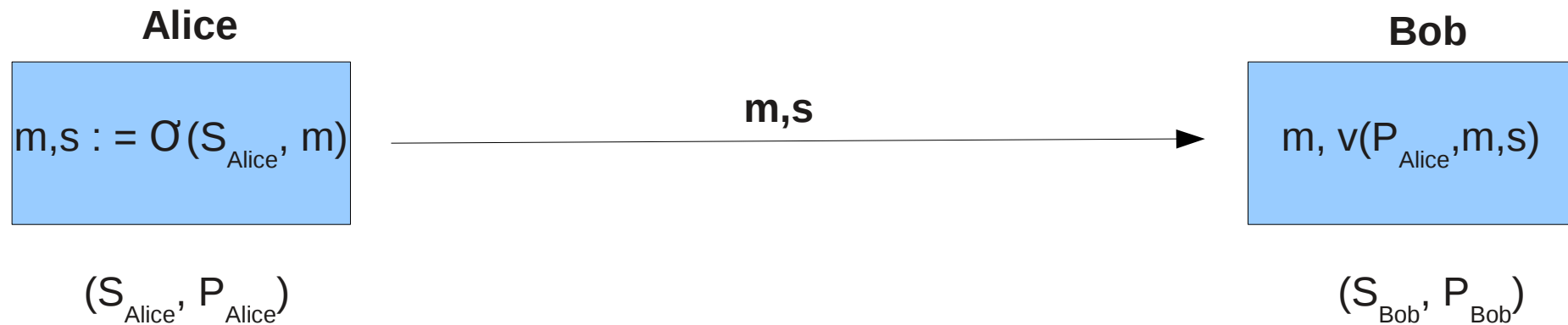
Input

Hash sum.

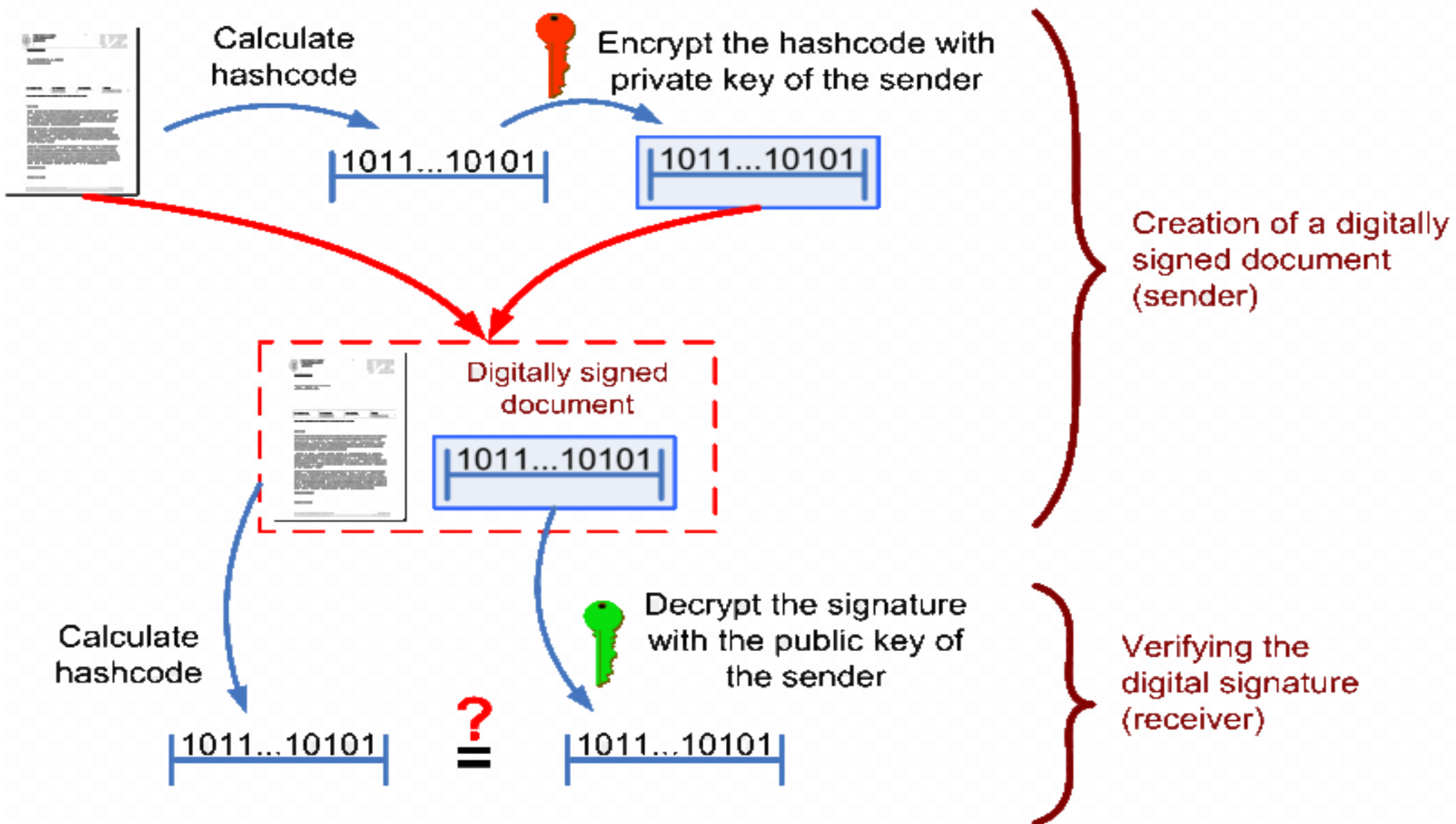


One Way Function

Digital Signatures



Creating and verifying a digital signature



If the calculated hashcode does not match the result of the decrypted signature, either the document was changed after signing, or the signature was not generated with the private key of the alleged sender.

Summary of Cryptography

Secret key Cryptography:

- It uses a single key for both encryption and decryption processes
- Since single key is used for both encryption and decryption , it is also called as Symmetric Encryption

Public key Cryptography:

- It uses one key for encryption and another for decryption
- One key is designated as a public key which is open to public and the other key is designated as a private key which is kept secret

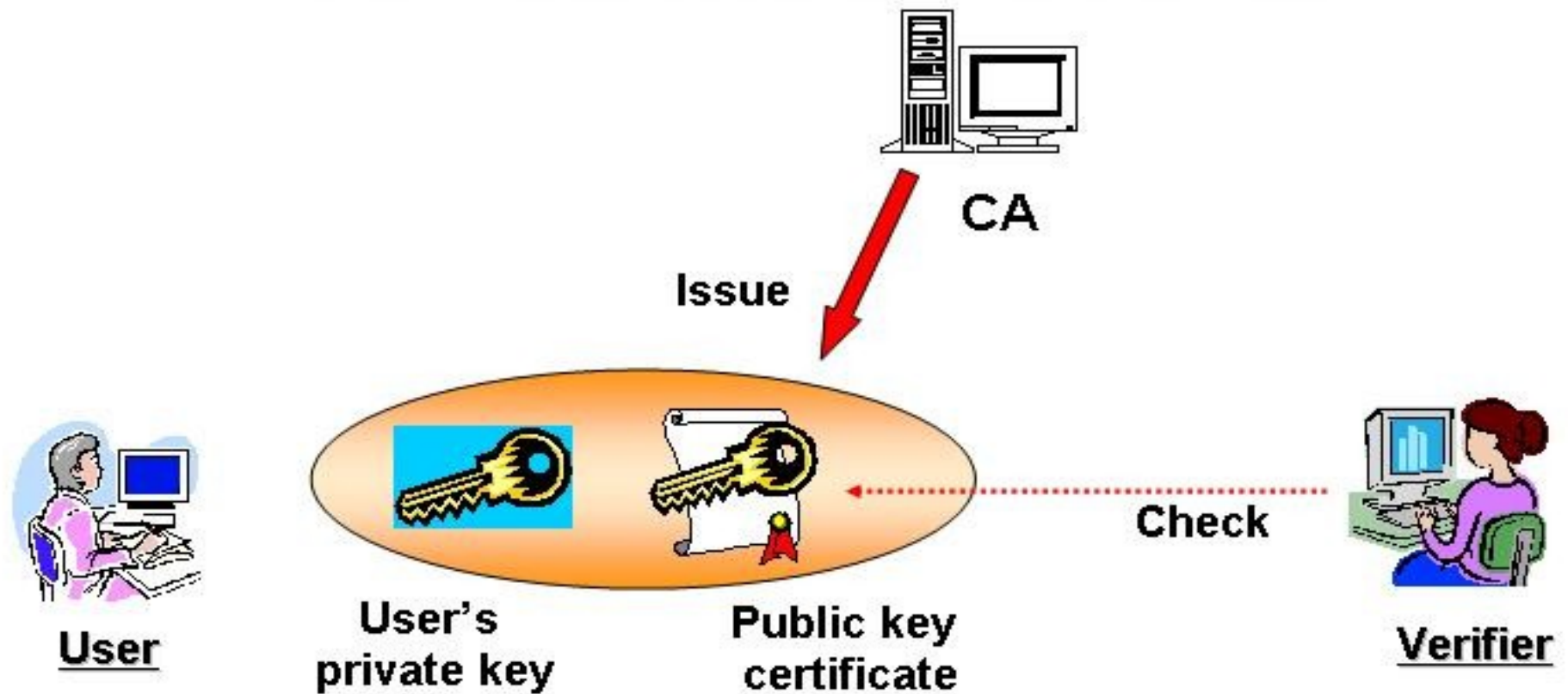
Hash Functions:

- It uses a mathematical transformation to irreversibly "encrypt" information
- It is also called 'Message Digest' and One-way Encryption, are algorithms that, in some sense, use no key
- Instead, a fixed-length hash value is computed based upon the plaintext
- Hash algorithms are typically used to provide a *digital fingerprint* of a file's contents

Trivia Quiz

How do I find Bob's public key?

Public Key Infrastructure (PKI)



Register once, use everywhere

Problems with PKI

- CA must be trusted by everyone

- Liability

Home > Security > News



Hacked certificate authority DigiNotar goes out of business

Dutch company announces bankruptcy

By Tim Greene | [Network World US](#) | Published 11:41, 21 September 11

The theft of SSL certificates from Dutch certificate authority

DigiNotar so undermined trust in the company that it has gone bankrupt.

Responsible for taking down the company is a single attacker, believed to be in Iran, who stole more than 500 certificates used to authenticate sites that make secure connections via SSL. DigiNotar was the primary certificate authority used by the Dutch government.

DigiNotar filed for bankruptcy yesterday and a Dutch court approved the filing today. Trustees were appointed to liquidate its assets, according to a statement by DigiNotar's parent company, Vasco.

The industry has been running from DigiNotar since the breach was made public August 29, more than two months after the company discovered an attack. Microsoft has blacklisted all DigiNotar digital certificates, deeming them untrusted. Google and Mozilla had already blacklisted the company's certificates, and the TOR project has recommended rejecting all DigiNotar certificates.

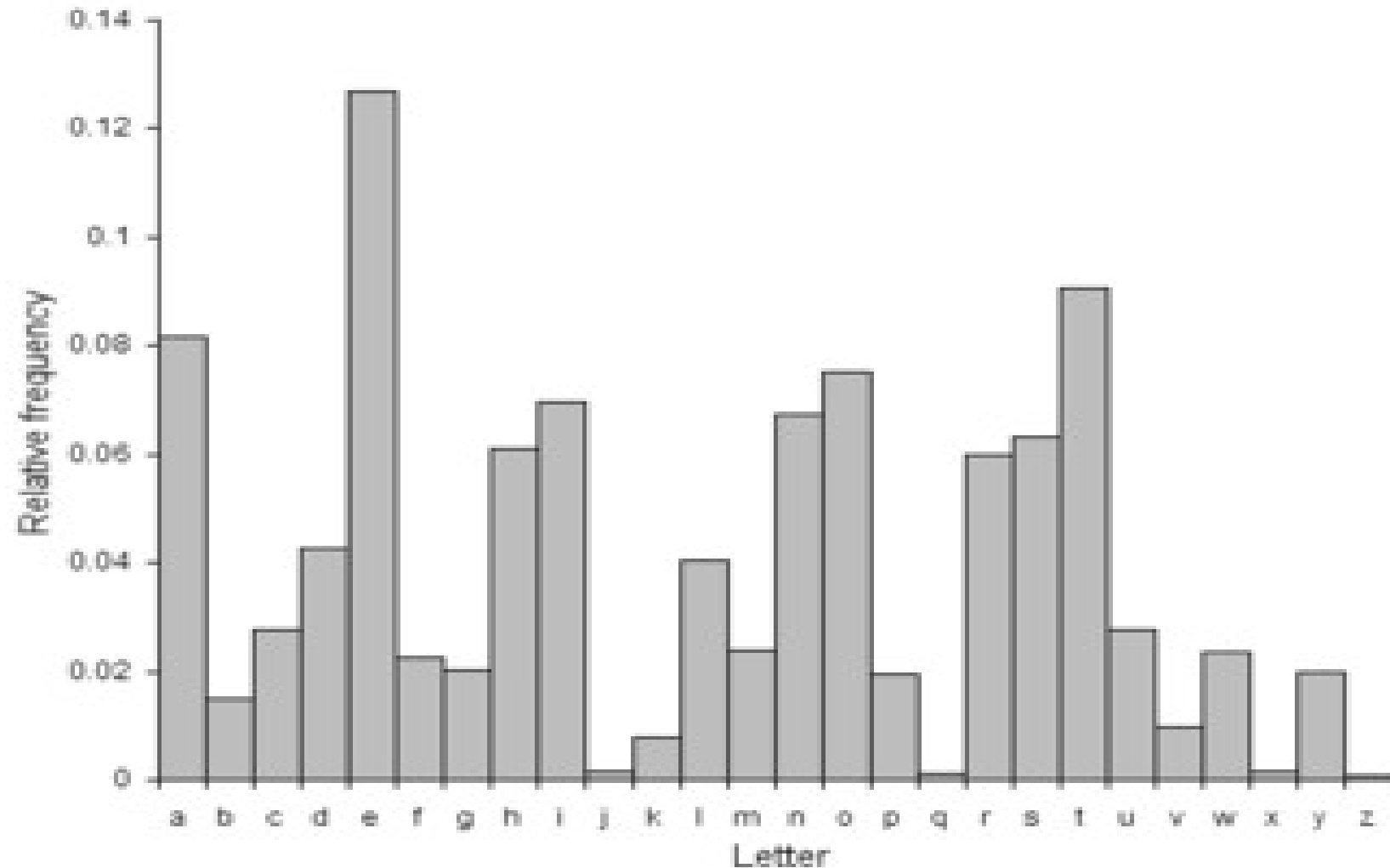
<http://bit.ly/OKAMA0>

Cryptanalysis

- Breaking the code without knowing the key
- Approaches
 - Frequency analysis
 - Certain letters of the alphabet appear more frequently than others
 - In English, “E” is one of the most frequent character used
 - Relies in statistics and linguistic
 - Brute Force
 - Trying every possible combination
 - Takes *some* time for complex algorithm
 - Using distributed system will help



Frequency Analysis



1. e (390395169, 12.575645%)
2. t (282039486, 9.085226%)
3. a (248362256, 8.000395%)
4. o (235661502, 7.591270%)
5. i (214822972, 6.920007%)
6. n (214319386, 6.903785%)
7. s (196844692, 6.340880%)
8. h (193607737, 6.236609%)
9. r (184990759, 5.959034%)
10. d (134044565, 4.317924%)

1. the (59623899, 3.508232%)
2. and (27088636, 1.593878%)
3. ing (19494469, 1.147042%)
4. her (13977786, 0.822444%)
5. hat (11059185, 0.650715%)
6. his (10141992, 0.596748%)
7. tha (10088372, 0.593593%)
8. ere (9527535, 0.560594%)
9. for (9438784, 0.555372%)
10. ent (9020688, 0.530771%)

1. th (92535489, 3.882543%)
2. he (87741289, 3.681391%)
3. in (54433847, 2.283899%)
4. er (51910883, 2.178042%)
5. an (51015163, 2.140460%)
6. re (41694599, 1.749394%)
7. nd (37466077, 1.571977%)
8. on (33802063, 1.418244%)
9. en (32967758, 1.383239%)
10. at (31830493, 1.335523%)

1. that (8709261, 0.761242%)
2. ther (6916008, 0.604501%)
3. with (6565513, 0.573866%)
4. tion (6314428, 0.551919%)
5. here (4285164, 0.374549%)
6. ould (4232202, 0.369920%)
7. ight (3540253, 0.309440%)
8. have (3324067, 0.290544%)
9. hich (3252540, 0.284292%)
10. whic (3247213, 0.283826%)

Brute Force Attack

PDF Password Cracker Pro

Encrypted PDF File: search-engine-optimization-starter-guide.pdf **Load** Decrypt

Type of attack: Brute-force

Brute-force range options

- ☒ All caps latin (A-Z)
- ☒ All small latin (a-z)
- ☒ All digits (0-9)
- ☒ All special symbols (!@...)
- ☒ Space
- ☐ All printable
- ☐ User defined characters

Minimal password length = 1 Characters

Maximal password length = 4 Characters

Start from: 123

End at:

Dictionary options

Dictionary file path:

Load d:\Program Files\PDF Password Cracker Pro v3.1\password.dic

☐ Try all possible upper/lower case combinations

Current password: Brute-force OK: password=123, key=F1 B1 C4 CF 72 13 60 D6 15 A5 EB E2

Tried passwords: Tried 1 passwords

Time spend: 0ms (0.0000s, 0.00m, 0.00h, 0.00d)

Start Stop Close About Purchase View Log

Project RC5

The "Bovine" RC5 effort was formed to take the responsibilities of coordinating and maintaining the RC5 servers that are needed to distribute key blocks to work on to all of the participating client programs. We depend heavily (entirely) on the participation of people like yourself, as we intend to solve this project via the use of brute force, trying every possible key there is.



We know this method works! On 19 October 1997 at 1325 UTC, [we found the correct solution](#) for the [RSA Labs](#) 56-bit secret-key challenge ([RC5-32/12/7](#)). The key was 0x532B744CC20999, and it took us 250 days to locate.

Then, on 14 July 2002 at 0150 UTC we [found the winning key](#) for the RSA Labs 64-bit secret-key challenge ([RC5-32/12/8](#)). That key was 0x63DE7DC154F4D039 and took us 1,757 days to locate. As of 03 December 2002, we're now working on the 72-bit RSA Labs secret-key challenge ([RC5-32/12/9](#)). In summary:

- RC5-56: 'The unknown message is: It's time to move to a longer key length'
- RC5-64: 'The unknown message is: Some things are better left unread'
- **RC5-72: ??? (In progress; you can help!)**

In May 2007, RSA Labs announced that Secret Key Challenge would be discontinued. Fortunately, due to the continued interest in our RC5-72 project we have decided to privately sponsor the prize and operate the RC5-72 project as before. You can read about this in [bovine's 2008-Sep-08 plan](#) and in [bovine's 2007-May-21 plan](#).

Current speeds and statistics for individual participants or teams are available at our [dedicated stats server](#). You can find out our current overall speed for the entire network at our [network status page](#).

If you have any technical support questions regarding the operations of your distributed.net client, then please click here to send mail to help@distributed.net. Be sure to also check out the [FAQ-o-Matic](#) to see if your question has already been answered.

The Prize

[RSA Labs](#) was offering a US\$10,000 prize to the group that wins this contest. The distribution of the cash was to be as follows:

- \$1000 to the winner
- \$1000 to the winner's team (or to the winner if not on a team)
- \$6000 to a non-profit organization chosen by all participants
- \$2000 to distributed.net for building the network and supplying the code

The recipient non-profit is chosen by means of a meritocratic vote through an extension of the stats database. We will [distribute the RC5-72 prize money](#) based on your votes, with one vote per workunit per person. You can also see how we've distributed the prize money on previous RC5 projects: [RC5-56](#) and [RC5-64](#)



Projects

— RC5

— OGR

Download

News

Help/Support

Discussion

Bug Database

Source Code

Research

Statistics

.plans/blogs

Corporate Info

Press Room

History

DnetWare Store

Donations

Credits

Find on this site:

Search



Moo.

[Get the client](#)

Code crackers break 923-bit encryption record

In what was thought an impossibility, researchers break the longest code ever over a 148-day period using 21 computers.



by [Dara Kerr](#) | June 20, 2012 5:41 PM PDT

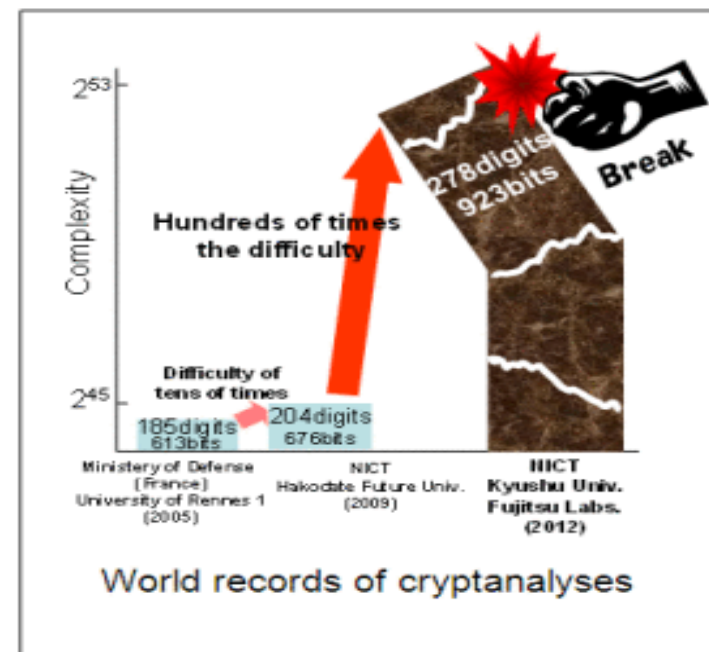


Before today no one thought it was possible to successfully break a 923-bit code. And even if it was possible, scientists estimated it would take thousands of years.

However, over 148 days and a couple of hours, using 21 computers, the code was cracked.

Working together, Fujitsu Laboratories, the National Institute of Information and Communications Technology, and Kyushu University in Japan announced today that they broke the world record for cryptanalysis using next-generation cryptography.

"Despite numerous efforts to use and spread this cryptography at the development stage, it wasn't until this new way of approaching the problem was applied that it was proven that pairing-based cryptography of this length was fragile and could actually be broken in 148.2 days," Fujitsu Laboratories wrote in a [press release](#).



(Credit: Fujitsu Laboratories)