UNIVERSITÉ LIBRE DE BRUXELLES,
UNIVERSITÉ D'EUROPE

ULB

FACULTY OF SCIENCES
COMPUTERSCIENCES DEPARTMENT

INFO-F-405: Introduction to cryptography

Misuse of encryption

GROUP 9

DEPUYDT Antoine
FISHEL David
KAGRAMANYAN George
MUDURA Mircea
ORINX Cédric
VAN EETVELDT Jordan

Academic year 2016-2017

Contents

1 Introduction

sudo apt-get install texlive-lang-cyrillic

2 Conclusion

Appendices

A Decrypted Messages (group 9)

A.1 Message A

Vienna is the capital of Austria. It is one of its largests cities.
Vienna is 410 square kilometers, almost 2 million people live there.
Vienna is situated in the Eastern part of Austria, it is standing on Danube river.
Vienna is in the UTC+1 time zone.
When tourists come to Vienna they often visit Schönbrunn Palace, Austrian Parliament,
City Hall, and St. Stephen's Cathedral.
Do not forget to go to opera when you visit Vienna.

A.2 Message B

Shame on you! Shame, shame, shame! What are you trying to do? Are you trying to break my cryptosystem?
Do you know that reading other people's letters is not very nice and not polite?
I am not doing that knind of things!
Who on earth gets into my personal life like that? And why are you doing it?
Is someone forcing you? No? If not, then what the hell is wrong with you?
My messages to Alice are strictly confidential! Only me, Alice and the NSA can read this e-mails..
So, dear hacker, stop it right now!
Best regards,
Eve.

A.3 Message C

Man, cartoons are the best! I like Futurama.
It is a sci-fi show about future. The story turns around a guy from the 20th century
who was frozen for many years and then he wakes up in a crazy future!
They have created 7 seasons and every one of them is just great!
They have so many fun characters, professor Farnsworth, Doctor Zoiberg, Leela
and a robot called Bender! You should watch it!

A.4 Message D

Scholars agree that classical information are an interesting new topic in the field of e-voting technology, and electrical engineers concur. In this work, we prove the visualization of information retrieval systems. In order to fix this obstacle, we verify not only that Scheme and Markov models are largely incompatible, but that the same is true for the World Wide Web.

A.5 Message E

Leading analysts agree that electronic communication are an interesting new topic in the field of theory, and cyberinformaticians concur. After years of confusing research into scatter/gather I/O, we prove the visualization of write-ahead logging. Of course, this is not always the case. Moth, our new application for voice-over-IP, is the solution to all of these obstacles.

A.6 Message F

The implications of multimodal algorithms have been far-reaching and pervasive. Given the current status of concurrent technology, information theorists obviously desire the deployment of replication, which embodies the private principles of cyberinformatics. In this position paper we introduce a novel application for the analysis of RAID (Tamkin), proving that Internet QoS and IPv4 can collaborate to fulfill this objective.

A.7 Message G

Local-area networks and autonomous epistemologies have been extensively synthesized by cyberneticists. It should be noted that Gob controls hierarchical databases. Existing mobile and real-time heuristics use client-server modalities to explore large-scale theory. While conventional wisdom states that this issue is generally addressed by the development of the Internet, we believe that a different method is necessary. In the opinions of many, we view networking as following a cycle of four phases: refinement, creation, simulation, and creation. Thus, we concentrate our efforts on proving that the partition table and e-business are generally incompatible.

A.8 Message H

Мать с младенцем спасена;
Землю чувствует она.
Но из бочки кто их вынет?
Бог неужто их покинет?
Сын на ножки поднялся,
В дно головкой уперся,
Понатужился немножко:
"Как бы здесь на двор окошко
Нам проделать?" - молвил он,
Вышиб дно и вышел вон.
Мать и сын теперь на воле;
Видят холм в широком поле;
Море синее кругом,
Дуб зеленый над холмом.
Сын подумал: добрый ужин
Был бы нам, однако, нужен.
Ломит он у дуба сук
И в тугой сгибает лук,
Со креста снурок шелковый
Натянул на лук дубовый,
Тонку тросточку сломил,
Стрелкой легкой завострил
И пошел на край долины
У моря искать дичины.

A.9 Message I

UHlelo Lobhalomfihlo kuyikhono ukukhuluma phambi sophikisana. Lokhu isayensi kuyisisekelo of security computer zanamuhla. Abacwaningi Security ukudala ezokuphepha ubuchule. Kukhona ubuchule eziningi ezinjalo, owaziwa kakhulu kuba ukubethela. Ukubethela isinika ithuba ukudlulisa ulwazi oluyimfihlo.

A.10 Message J

Trust I seek and I find in you
'Cause you know I'm here for you
Body's aching all the time
Reaching a fever pitch
Ignite the light
To seize everything you ever wanted
It's such a feelin' that my love
You're in control just like a child
My worst distraction, my rhythm and blues