ULB UNIVERSITÉ LIBRE DE BRUXELLES

INFO-F405 – Computer Security

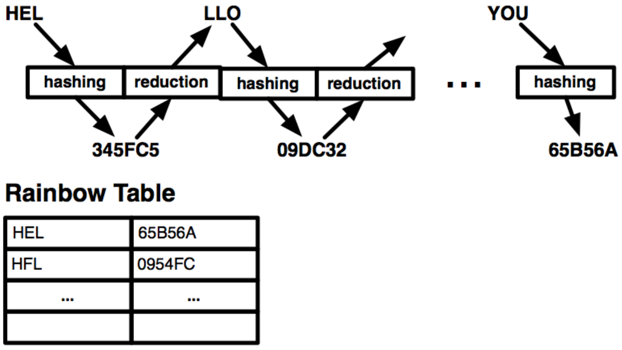
Project 1 : Rainbow Tables

Anthony Debruyn, Brian Delhaisse,
Alexis Lefebvre and Aurélien Plisnier.

Academic year 2013 - 2014

1 Introduction

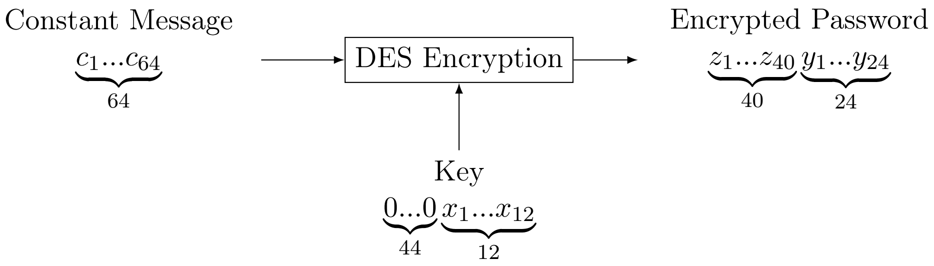
The project[1] for the course "Computer Security", for this year, consists of implementing a rainbow table. This project will be implemented in C++/Java.



HEL	65B56A
HFL	0954FC
...	...

Figure 1: Sequence of reductions and hashing, and the associated rainbow table. [2]

1.1 The hashing algorithm


Constant Message
$\underbrace{c_1...c_{64}}_{64}$
DES Encryption
Encrypted Password
$\underbrace{z_1...z_{40}}_{40}\underbrace{y_1...y_{24}}_{24}$
Key
$\underbrace{0...0}_{44}\underbrace{x_1...x_{12}}_{12}$

$$\text{where} \begin{cases} x_1...x_{12} = \text{password to be hashed.} \\ y_1...y_{24} = \text{fingerprint (=hashed password).} \end{cases}$$

Figure 2: The hashing algorithm

1.2 The reduction function

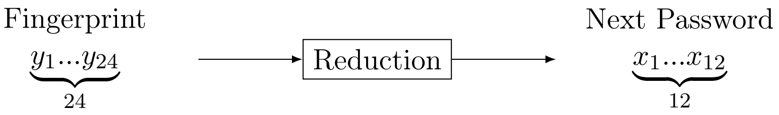

Fingerprint
$\underbrace{y_1...y_{24}}_{24}$
Reduction
Next Password
$\underbrace{x_1...x_{12}}_{12}$

Figure 3: The reduction function

[1] All further details about the project can be found on the "Université Virtuelle".

[2] Figure taken from the project brief made by the assistant Naïm Qachri.

2 The reduction functions

2.1 1th reduction function

2.2 2nd reduction function

2.3 3rd reduction function

2.4 4th reduction function

3 Conclusion