Homework 3

YueLi

15620161152260

Q1

```
# install stuff for hash calculation
install.packages("digest", repos='http://cran.us.r-project.org')
# call the library doing the hashes
library("digest")
# now do the hash code calculation
digest("I learn a lot from this class when I am proper
listening to the professor“,”sha256”)
digest("I do not learn a lot from this class when I am absent
and playing on my Iphone“,”sha256”)
```

Q2 Digital Signature Algorithm

- Yue Li

1. DSA Overview

- • Defination

- The Digital Signature Algorithm (DSA) is a Federal Information Processing Standard for digital signatures.

- (A digital signature is a mathematical scheme for demonstrating the authenticity of digital messages or documents.)

- • Remark:

- – Published in 1992

- – Sometimes called DSS (Digital Signature Standard)

2. Key generation

Key generation has two phases.

- The first phase is a choice of algorithm parameters which may be shared between different users of the system
- The second phase computes public and private keys for a single user.

3. Sensitivity

• With DSA, the entropy, secrecy, and uniqueness of the random signature value are critical.

• It is so critical that violating any one of those three requirements can reveal the entire private key to an attacker.

• Using the same signature value twice (even while keeping it secret), using a predictable value, or leaking even a few bits of it in each of several signatures, is enough to reveal the private key.

4. DSA Remark

- Advantages:

– Suitable to storage limited device

– Hashing function is used

– Based on discrete logarithm problem

- Disadvantage:

– Unpublicized selection

Q3

- #20171017 JSON input from CRIX , trial done in XMNinstall.packages("rjson",repos="http://cran.us.r-project.org")
- library("rjson")
- ==========
- # create and save in txt（save as ″try.json″ ; ″all types″ ;）
- {
- "ID":["001","002","003","004","005","006","007","008"],
- "Salary":["600","500","600","700","800","500","600","70"],

- "StartDate":["1/1/2016","9/23/2017","11/15/2017","5/11/2017,"3/27/2017","5/21/2017",
- "7/30/2016","6/17/2016"],
- }
- ==========

- install.packages("rjson")
- # Load the package required to read JSON files.
- library("rjson")
- # Give the input file name to the function.
- result <- fromJSON(file = “try.json")
- # Print the result.
- print(result)

Q4

- Q4 #from professor

- #20171017 JSON input from CRIX , trial done in XMNinstall.packages("rjson",repos="http://cran.us.r-project.org")
- library("rjson")
- json_file = "http://crix.hu-berlin.de/data/crix.json"
- json_data = fromJSON(file=json_file)
- crix_data_frame = as.data.frame(json_data)
- x = crix_data_frame
- n = dim(x)
- a = seq(1,n[2],2)
- b = seq(2,n[2],2)
- date = t(x[1,a])
- price = t(x[1,b])
- plot(price)
- dim(price)
- ts.plot(price)
- ret = diff(log(price))
- ts.plot(ret)