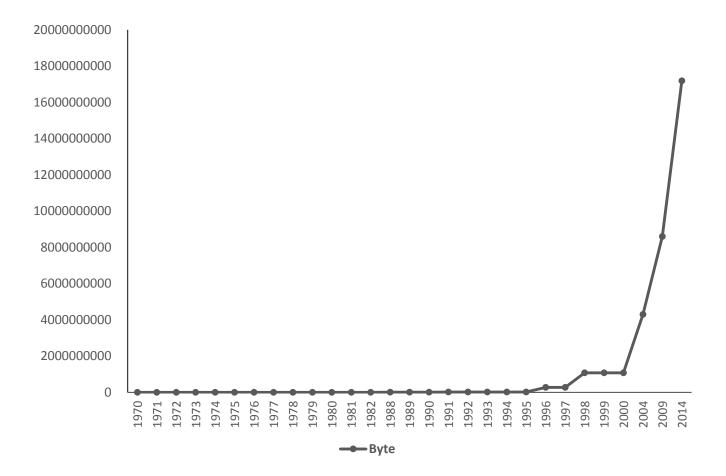
HW Unit 1

By: Qian Liu

15620161152269

Year	Byte
1970	262144
1971	262144
1972	262144
1973	262144
1974	262144
1975	262144
1976	262144
1977	262144
1978	262144
1979	262144
1980	262144
1981	262144
1982	262144
1988	2097152
1989	2097152

Year	Byte
1990	2097152
1991	16777216
1992	16777216
1993	16777216
1994	16777216
1995	16777216
1996	268435456
1997	268435456
1998	1073741824
1999	1073741824
2000	1073741824
2004	4294967296
2009	8589934592
2014	17179869184



Logistic regression

Logistic regression is used in various fields, including machine learning, most medical fields, and social sciences.

Logistic regression may be used to predict whether a patient has a given disease (e.g. <u>diabetes</u>; <u>coronary heart disease</u>), based on observed characteristics of the patient (age, sex, <u>body mass index</u>, results of various <u>blood tests</u>, etc.).

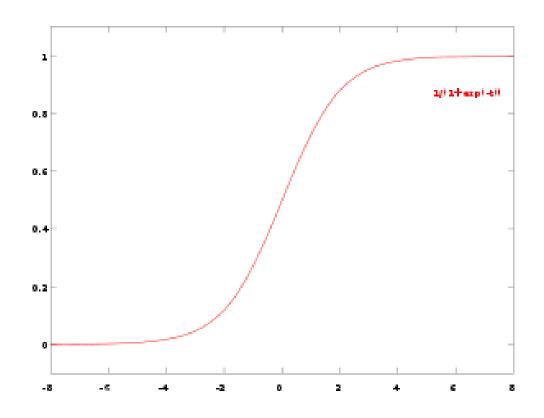
Another example might be to predict whether an American voter will vote Democratic or Republican, based on age, income, sex, race, state of residence, votes in previous elections, etc.

Stata

logistic hcv age marry sex

Different from GLM

• Dependent variable: "0" or "1", not cardinal numbers.



HW Unit 2

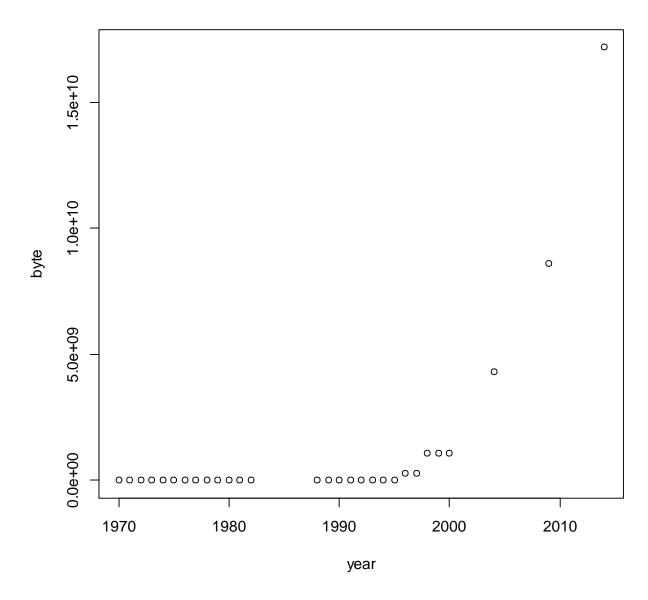
By: Qian Liu

15620161152269

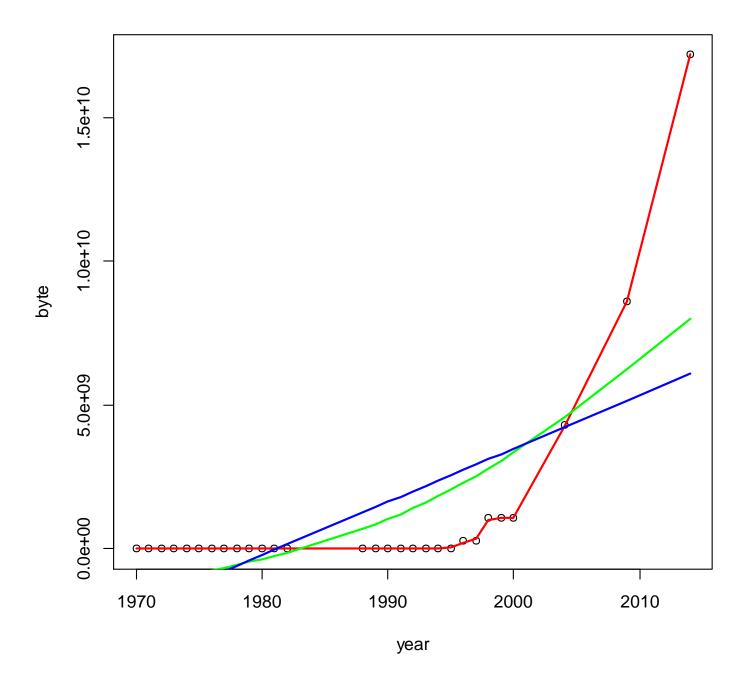
>year=c(1970,1971,1972,1973,1974,1975,1976,1977,1978,1979,1980,1981,1982,1988,1989, 1990,1991,1992,1993,1994,1995,1996,1997,1998,1999,2000,2004,2009,2014)

>byte=c(262144,2

> plot(year,byte)



```
>year=c(1970,1971,1972,1973,1974,1975,1976,1977,1978,1979,1980,1981,1982,1988,1989,
1990.1991.1992.1993.1994.1995.1996.1997.1998.1999.2000.2004.2009.2014)
>byte=c(262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,262144,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,2621444,26214444,2621444,2621444,2621444,2621444,26214444,2621444,2621444,2621444,2621444,262144444
2144,262144,262144,2097152,2097152,2097152,16777216,16777216,16777216,
16777216,268435456,268435456,1073741824,1073741824,1073741824,4294967296,85899
34592,17179869184)
> plot(year,byte)
> splines.reg.1= smooth.spline(x = year, y = byte, spar = 0.2)
> splines.reg.2 = smooth.spline(x = year, y = byte, spar = 1)
> splines.reg.3= smooth.spline(x = year, y = byte, spar = 2)
> plot(year,byte)
> lines(splines.reg.1, col = "red", lwd = 2)
> lines(splines.reg.2, col = "green", lwd = 2)
> lines(splines.reg.3, col = "blue", lwd = 2)
```



3.1Suppose you observe that in n=1000 mails (in 1 week) you have about 2 scams. Use the LvB /Possion pdf to calculate that you have 6 scam emails in 2 weeks.

3.2In Scammyland you have 5 scams on average, what is the probability to have no scammail.

3.1 R code:

> lambda=2

> x = 3

> dpois(x,lambda)

3.2 R code:

> lambda=5

> x = 0

> dpois(x,lambda)

HW Unit 3

By: Qian Liu

15620161152269

- > install.packages("digest", repos='http://cran.us.r-project.org')
- > library("digest")
- > sentence1=digest("I learn a lot from this class when I am proper listening to the professor", "sha256")
- > sentence2=digest("I do not learn a lot from this class when I am absent and playing on my Iphone", "sha256")
- > sentence1
- [1] "c16700de5a5c1961e279135f2be7dcf9c187cb6b21ac8032308c715e1ce9964c"
- > sentence2
- [1] "2533d529768409d1c09d50451d9125fdbaa6e5fd4efdeb45c04e3c68bcb3a63e"

2. Make 3-5 slides (in PPTX) on the DSA (Digital Signature Algorithms)

A **digital signature** is a mathematical scheme for demonstrating the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (<u>authentication</u>), that the sender cannot deny having sent the message (<u>non-repudiation</u>), and that the message was not altered in transit (<u>integrity</u>).

Digital signatures are often used to implement <u>electronic signatures</u>, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, <u>Turkey</u>, <u>India</u>, Brazil, Indonesia, <u>Mexico</u>, Saudi Arabia, <u>Switzerland</u> and the countries of the <u>European Union</u>, electronic signatures have legal significance.

2.



鲍勃



鲍勃的公钥





3.



苏珊

"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"



公钥加密

HNFmsEm6Un BejhhyCGKO **KJUxhiygSBC** EiC0QYIh/Hn 3xgiKBcyLK1 UcYiYlxx2lCF HDC/A



鲍勃



HDC/A

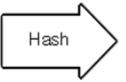
私钥解密



"Hey Bob, how about lunch at Taco Bell. I hear they have free refills!"

Trade crews of 160 diety Good Inverse a publisher First the createst of NGC Greety Count Provincy, a publishery contribution and contribution positions for the protections of allocations at mill. State PGC was published documentably as there was in hard of 1975, it has up mad drap shall be all over the world, and has state the rest hard wealther for published a translated for exceptions of it mad, whenting measurementable by the state of the published provided doug the resp. And there years I was the warpen at a create at an energy state by the UN Courteent Secretar, who contributed the term was translated when when DGC symmed on third the UN That its verying time was closed without indictance it in January 1975.

Comparing more de relayed in order back in World War I society to break colors. Children's proofs (id) not have worse to comparing the source stay were now in Amabar and the opposition. Solars people portained that their would retreat to a reset for some that held above, comparing in the constitution of the stay people. mental array have a need for energoine. Some of the preventioner's either hower upplying highly being more homed in their period, and to serve the old effective tensor companies. You served contrary people need to have usual to good cryptography:



Digest

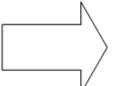
Digest



Signature

Digital Signature

Signature



The the creates of RGP directly Good Provings, a published econopsion actives a pushey for the protection of electronic mail. Since RGP was published documentarly as the create in June of 1995, it has a proving equal to true the receil, and has create became the fit hade receilable of endough for energy from oil 5 mail, waveling assessment inhabity are well of long for may fire them your I may for wagness or creates it in margination by the DM Courses Senter, who cannot not that have were broken when RGP species on that the Vernigation of the Course for the that the Vernigation was closed without indicates at in January 1995.

Compaines were developed in accordance in World Whe B scrainly be break codes. Ordinary propined in our brice wases to compaine the codes of the same state to the property of the code of the code of the Some people particulated that them moved overtile a read for motion than both a distribution of the code of the code of the social people would save be have a code for exception because it for exception when a distribution of the compaines. Some of the grandmant of a code of the same of the code of the same of the same of the period. And to write the old estimated in contact compare the Why would be code of the same of the same to Why would excit any people need to have a sense to good cryptography?

Signature

8.

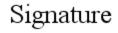
Signature

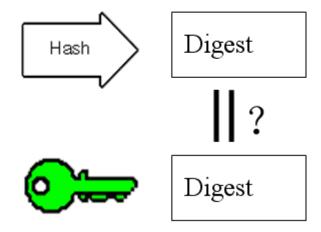


Digest

First the creates of FGP directly Good Proversit, a publishery encomposite activents purhays the the protections of electronic enail. State FGP was published connectionly as the event in force of 1993, I have greated organised by all over the receil, and has a chord became the fix hathe weedlands described for or cryption of 5 mails variety assumes to labeling the receipt of the fixed providing assumes to labeling the receipt of the fixed proof of the receipt of a creater of a mergentian by the DN Customer Service, who assumes that have even broken when FGP appead on this the US. That its verification was closed without indications t in factority 1995.

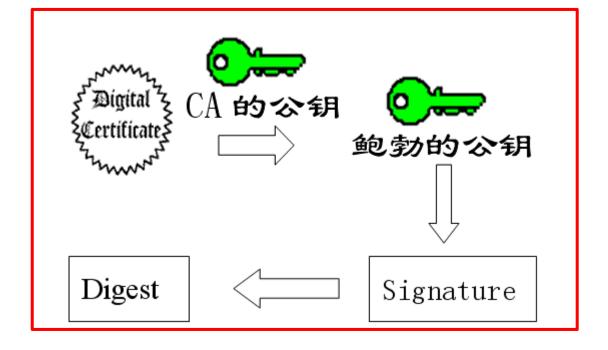
Computers more developed to secret back in World War Exactely to break colors. Collinary people (3) and have some to strangulary because they were here in further and to expend the Some people portion of the thore would return be a race for some that both down computers in the country, and some and that exist any people result serves have a reset for exception. Seems of the generalized formed serves have a reset for exception. Seems of the generalized for elimite toward upy tings right below were becomed in facility period, and have seen the old estimates toward contributes toward contributes the old estimates toward origins and they seem a centurary people seems.





Certificate Authority(CA)

Digital Certificate(DC)

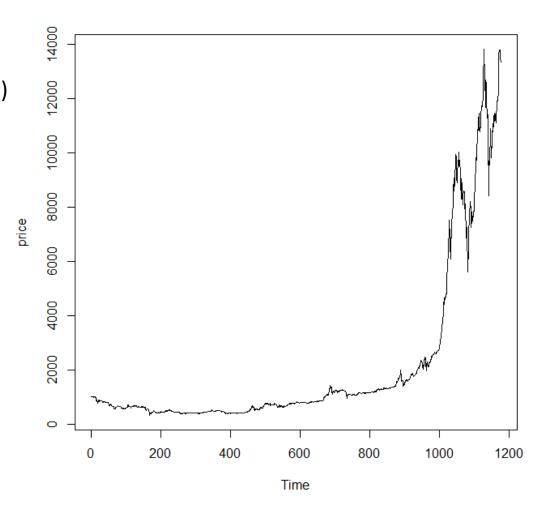


Let H be the hashing function and m the message:

- ullet Generate a random per-message value k where 1 < k < q
- Calculate $r = (g^k \mod p) \mod q$
- ullet In the unlikely case that r=0, start again with a different random k
- Calculate $s = k^{-1} \left(H\left(m \right) + xr \right) \bmod q$
- ullet In the unlikely case that s=0, start again with a different random k
- The signature is (r,s)
- Reject the signature if 0 < r < q or 0 < s < q is not satisfied.
- Calculate $w = s^{-1} \mod q$
- Calculate $u_1 = H(m) \cdot w \mod q$
- Calculate $u_2 = r \cdot w \mod q$
- Calculate $v = (g^{u_1}y^{u_2} \mod p) \mod q$
- The signature is invalid unless v=r

```
> install.packages("rjson",repos='htpp://cran.us.r-project.org')
> library("rjson")
> name<-c("Bob","Jon","Linda","Kim","Susan","Amy")
> gender<-c("M","M","F","M","F","F" )
> individualfeature<-data.frame(name,gender)
> data<-as.matrix( individualfeature)
> cat(toJSON(data))
["Bob","Jon","Linda","Kim","Susan","Amy","M","M","F","M","F","F"]
```

```
> install.packages("rjson",repos='htpp://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])
> ts.plot(price)
```



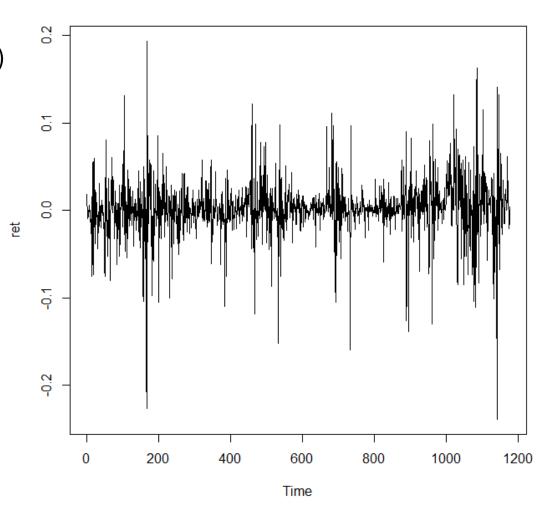
HW Unit 4

By: Qian Liu

15620161152269

```
>libraries = c("ccgarch", "rmgarch", "xts", "zoo")
>lapply(libraries, function(x) if (!(x %in% installed.packages())) { install.packages(x) })
>lapply(libraries, library, quietly = TRUE, character.only = TRUE)
>load(file = "crix.RData")
>load(file = "ecrix.RData")
>load(file = "efcrix.RData")
>ecrix1 = zoo(ecrix, order.by = index(crix1))
>efcrix1 = zoo(efcrix, order.by = index(crix1))
>my.panel <- function(x, ...) {
 lines(x, ...)
 lines(ecrix1, col = "blue")
 lines(efcrix1, col = "red") }
>plot.zoo(crix1, plot.type = "multiple", type = "l", lwd = 1.5, panel = my.panel, main = "Indices in the CRIX family")
```

```
> install.packages("rjson",repos='htpp://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])
> ts.plot(price)
> ret=diff(log(price))
> ts.plot(ret)
```



```
# install and load packages
>libraries = c("zoo", "tseries", "xts")
>lapply(libraries, function(x) if (!(x %in% installed.packages())) { install.packages(x) })
>lapply(libraries, library, quietly = TRUE, character.only = TRUE)
# load dataset
>load(file = "crix.RData")
# histogram of returns
>hist(ret, col = "grey", breaks = 20, freq = FALSE, ylim = c(0, 25), xlab = NA)
>lines(density(ret), lwd = 2)
>mu = mean(ret)
>sigma = sd(ret)
>x = seq(-4, 4, length = 100)
>curve(dnorm(x, mean = mean(ret), sd = sd(ret)), add = TRUE, col = "darkblue", lwd = 2)
# qq-plot
>ggnorm(ret)
>ggline(ret, col = "blue", lwd = 3)
```

```
> install.packages("rjson",repos='htpp://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])
> ts.plot(price)
> ret=diff(log(price))
> ts.plot(ret)
# plot of pacf
>autopcorr=pacf(ret,lag.max=20,ylab="Sample Partial Autocorrelation",main=NA,ylim=c(-0.3.0.3),lwd=2)
>print(cbind(autopcorr$lag, autopcorr$acf))
```

```
# arima202 predict
>fit202 = arima(ret, order = c(2, 0, 2))
>crpre = predict(fit202, n.ahead = 30)

>dates = seq(as.Date("02/08/2014", format = "%d/%m/%Y"), by = "days", length = length(ret))
>plot(ret, type = "l", xlim = c(0, 644), ylab = "log return", xlab = "days", lwd = 1.5)
>lines(crpre$pred, col = "red", lwd = 3)
>lines(crpre$pred + 2 * crpre$se, col = "red", lty = 3, lwd = 3)
>lines(crpre$pred - 2 * crpre$se, col = "red", lty = 3, lwd = 3)
```

```
# install and load packages
>libraries = c("FinTS", "tseries")
>lapply(libraries, function(x) if (!(x %in% installed.packages())) { install.packages(x) })
>lapply(libraries, library, quietly = TRUE, character.only = TRUE)
>setwd()
>load(file = "crix.RData")
>Pr = as.numeric(crix)
>Da = factor(date1)
>crx = data.frame(Da, Pr)
# plot of crix return
>ret = diff(log(crx$Pr))
>Dare = factor(date1[-1])
>retts = data.frame(Dare, ret)
```