March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable through the Math 103 home page for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable through the Math 103 home page with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

FBI group members

Edward DeGuzman `edsd@eden.rutgers.edu`
Kim Fife `hijumpkin@aol.com`
Alyna Jacobs `alynaj@eden.rutgers.edu`
Daniel Shaivitz `flynt@eden.rutgers.edu`

OVER

What to prepare for

You will write a supporting memo (at most 3 pages long) for a senior FBI official testifying before a committee of the U.S. Congress. The official has been asked to testify in support of a bill tightly regulating the sort of encryption software which can be sold or exported. Some points listed below may be helpful to you, but don't feel limited to them, please. See the website `http://www.fbi.gov/library/encrypt/encrypt.htm` and possibly find more support for your positions at the websites `http://www.nsa.gov/` and `http://www.cia.gov/`.

- Strong cryptography could help kidnappers by allowing secret communication between the criminals, and assisting synchronization of their actions.
- Strong cryptography easily available could assist international terrorists, who may be backed by rogue nations, use international communications and then local communications to target and execute their missions.
- Strong cryptography easily available could deter our efforts to protect the nation's information infrastructure, increasing the vulnerability of financial communications.

In your oral rebuttal

Be prepared to deal with the financial argument that restrictions on strong crypto domestically lead to decreased sales since residents of other countries can write software with good crypto. Also, export regulations of crypto software lead to de facto restrictions on what U.S. citizens are likely to be able to use inside the U.S. since there is, effectively, world-wide, one market for software, thereby regulating even what U.S. citizens are likely to be able to use inside the U.S.! Of course, be prepared to deal with arguments about civil liberties.

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable through the Math 103 home page for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable through the Math 103 home page with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

ACLU group members

Julie Anastasi	julana@eden.rutgers.edu
Nolan Henry	ndhenry@eden.rutgers.edu
Mark Ryan	digamma@eden.rutgers.edu
Margaret Wu	mjwu@eden.rutgers.edu

OVER

What to prepare for

You will write a memo (at most 3 pages long) supporting the testimony of an important ACLU official before a committee of the U.S. Congress. Your memo will outline an attack of the controls on crytptography that exist and on those that are proposed. The web page `http://www.aclu.org/issues/cyber/hmcl.html` should be your primary source. Various links can be followed from it (see, e.g., below). You may further choose to emphasize some of the items below but don't be limited by them.

- Controls on cryptography are censorship, plain, simple. The First Amendment protects U.S. citizens (and residents?).
- There's an inherent right to privacy in commercial transactions, a right to privacy in e-mail to friends, fellow workers, ...
- See `http://www.aclu.org/issues/cyber/priv/privpap.html` for a detailed discussion of some of these issues from the point of view of more classical civil liberties.

In your oral rebuttal

Be prepared to deal with arguments about criminals and terrorists, about economic pressures, and arguments about dealing with countries whose traditional "freedoms" relative to wiretapping, etc., are perhaps less comprehensive than our own. How would you deal with the question of whether suspected pornographers should be required to decrypt their files after satisfactory court action? There has been considerable debate about such matters in the U.S. and other countries.

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable <u>through the Math 103 home page</u> for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable <u>through the Math 103 home page</u> with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

Electronic Freedom group members

Craig Gargano `gargano@eden.rutgers.edu`
Amy Joh `ajoh@eden.rutgers.edu`
Hanna Schwartz `hls25@eden.rutgers.edu`
Miroslaw Szatko `mszatko@eden.rutgers.edu`

OVER

What to prepare for

You are preparing a position paper (at most 3 pages long) for an organization representing the viewpoint of a new subculture whose members believe that widespread and unrestricted use of electronic "stuff" will give us all better lives. They are perhaps more extreme than some traditional civil liberties folks, more attuned to what is possible to do with cryptography, and more willing to discuss the technical shortcomings and features of various policy issues. Sometimes the efforts of these folks seem to have a rather anti-U.S. orientation, declaring that U.S. policies are rather inferior to those (chosen from, say) policies of Western Europe. These webpages may be useful to you: `http://www.cdt.org/crypto/`, `http://www.eff.org/`, and `http://www.epic.org/crypto/`. Remark that money is on your side: if folks in the U.S. don't do it, the software will be available easily from people living in lots of other places.

In your oral rebuttal

Be prepared to deal with the accusation of uncaring irresponsibility: spies, terrorists, and criminals of all sorts could be aided by your efforts! An assertion could be made that "good" people will naturally agree with the sort of mild restrictions on e-commerce and communications proposed by (some) governments, since benefits will be gotten by "everyone".

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable through the Math 103 home page for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable through the Math 103 home page with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

Russia/fSU (former Soviet Union) group members

Michael Civins `mcivins@eden.rutgers.edu`
Jonathan Hammer `jrhammer@eden.rutgers.edu`
Peter Samet `psamet@eden.rutgers.edu`
Lee Walker `lcwalker@eden.rutgers.edu`

OVER

What to prepare for

You have a difficult task. You are to prepare a position paper (at most 3 pages long) for a meeting of an international organization (say, the International Telecommunications Union or an international trade organization) on the policies regarding use, import, and export of cryptographic machinery and software. You could try to represent the whole (rather heterogeneous) fSU area, or choose to discuss only one country (the obvious candidate being Russia itself). I'd like you to present a selection of the policies that U.S. people might find restrictive or strange. You are to be an advocate/defender of these policies. You may defend your policies regarding cryptography with a mixture of convenient logic, exaggeration, and history. Mention specific policies and give some comments to support these policies. For example, your comments could include (but not be limited by) reasons such as the following:

- Our traditions are not the same as those of Western Europe and North America, and we will not abandon our own culture and history.
- We have special (perhaps temporary!) needs for controlling security in communications, since we have been threatened historically by our neighbors, country X and country Y and ...
- Our resources have been exploited miserably by international corporations and we must be able to monitor communications to prevent possible future exploitation.
- Residents of our country must be willing to sacrifice some privacy so that our future will be better.

In your oral rebuttal

Be prepared to defend "your" country's positions. One classic style: throw accusations at the accusers. Remark that those who accuse you of controlling communications already have secure communications of their own, and are just trying to prevent others from enjoying similar security. Have a few facts which you cite in a very emotional manner.

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable <u>through the Math 103 home page</u> for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable <u>through the Math 103 home page</u> with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

European Union group members

Juraj Dlhopolcek `juraj@eden.rutgers.edu`
Sunit Jariwala `sunitj@eden.rutgers.edu`
Dan Ksepka `dksepka@eden.rutgers.edu`
Frank J. Miles `fjmiles@eden.rutgers.edu`

OVER

What to prepare for

You have a difficult task. You are to prepare a position paper (at most 3 pages long) for a meeting of an international organization (say, the International Telecommunications Union or an international trade organization) on the policies regarding use, import, and export of cryptographic machinery and software. You could try to represent the whole (rather heterogeneous) EU area, or choose to discuss only one or two countries. I'd like you to present a selection of the policies that U.S. people might find restrictive or strange. You are to be an advocate/defender of these policies. You may defend your policies regarding cryptography with a mixture of convenient logic, exaggeration, and history. Mention specific policies and give some comments to support these policies.

Note that the history of Western Europe with regard to laws and practices (what governments say and what they actually do) is complex. Look at the entries for France and Germany in `http://cwis.kub.nl/~frw/people/koops/cls2.htm` and consider this recent news report from `http://www.wired.com/news/politics/0,1283,34350,00.html`:

> 3:00 a.m. 16.Feb.2000 PST DUBLIN, Ireland – Britain is likely to become the first country in the world to make imprisonment a possible consequence of refusing to surrender, or even losing, one's private encryption keys.
>
> At the same time, neighboring Ireland is preparing legislation that would make it the first country to prohibit law enforcement from forcing encryption users to hand over their private keys.
>
> The new British law also would compel Internet service providers to build in "reasonable interception capabilities" to networks and could force ISPs to hand over data traffic information – email destinations, Web site visits, IP names – to law enforcement without a search warrant. It includes provisions for listening in on mobile and satellite phone calls, intercepting pager messages, and bugging office switchboards.
>
> The topsy-turvy state of affairs is emblematic of the approach of the two countries to electronic commerce legislation.

In your oral rebuttal

Be prepared to defend "your" country's positions. Assert that you are correct, distort history and economics judiciously if necessary to support your wishes, claim sovereign immunity, etc. Have a few facts ready if you absolutely need them!

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable through the Math 103 home page for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable through the Math 103 home page with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

Latin American group members

Adriana Garriga López `bjork@eden.rutgers.edu`
Derek Kanarek `ddk@eden.rutgers.edu`
Carlos Ron `carlosron@aol.com`

OVER

What to prepare for

Please present a position paper (at most 3 pages long) for a meeting of an international organization (say, the International Telecommunications Union or an international trade organization) on the policies regarding use, import, and export of cryptographic machinery and software. You could try to represent the whole (rather heterogeneous) Latin American area, or choose to discuss only one or two countries. Take a look at the references. Maybe send e-mail to embassies – the information I have found (on the web page `http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm` for example) is rather sketchy. See what you can develop, please.

I suspect that the laws and the practices of these governments might not be totally the same: that is, what the governments declare is legal and what they are willing to tolerate may be different. But I may be wrong. It would be interesting to get some information. What could a businessperson sending e-mail or keeping files have to face? Could the police demand the "keys" to a cryptosystem?

In your oral rebuttal

Of course be prepared to defend "your" country's positions. Assert that you are correct, distort history and economics judiciously if necessary to support your wishes, claim sovereign immunity, etc. Have a few facts ready if you absolutely need them!

March 5, 2000

RSA math & policy assignments

This assignment is complex and has three parts. I've divided the class into seven groups. You should all discuss how to share the work involved. Here is a description of your group's assignment:

Part 1: Communication using RSA

Each group will have to work on communicating using the RSA algorithm. Every member of the group should have received by e-mail the private/secret key for the group. Please see the webpage
`http://www.math.rutgers.edu/~greenfie/currentcourses/math103spring/rsa.html`
reachable through the Math 103 home page for exact information on what to do now, and get started as soon as possible.

Parts 2 & 3: Government Policy about Cryptography: a Debate and Papers

Your group will independently prepare and present for discussion an aspect of government policy about cryptography. There will be two grades: one for the oral presentation, and one for the written report. Guidelines for both are given below. The grades earned by the group will be the grades for each student in the group. The names of the people in each group are below. I've created a web page
`http://math.rutgers.edu/~greenfie/currentcourses/math103spring/gov_policy.html`
reachable through the Math 103 home page with a very limited number of links on this debate's topics. These topics are rather controversial and change is rapid. Discussion and information about them exist on many web pages.

Oral presentation

- Ten minutes to present the original position of the group.
- Five minutes to respond to questions (rebuttal).

Grades for the oral presentation will be based on the original presentation, the questioning of other presentations (take notes during the presentations of the other groups!), and the response to questioning in the rebuttal time.

Written report

Each group will hand in a policy paper at the class meeting following the oral presentations. I'll accept a preliminary version of the policy paper earlier for analysis and comment (and corrections!), if this is desired. If you consent, I will post your report as a web page linked to the course web page.

Far East group members

Helen Lloyd-Williams `hrlw@eden.rutgers.edu`
Yariv Sadan `yarivs@eden.rutgers.edu`
Kim Shah `kimushah@eden.rutgers.edu`

OVER

What to prepare for

Please present a position paper (at most 3 pages long) for a meeting of an international organization (say, the International Telecommunications Union or an international trade organization) on the policies regarding use, import, and export of cryptographic machinery and software. You can select from any (or all!) of your area, which certainly represents a very important part of the world, by many measurements (population, resources, industry, general economic strength, military power). You may wish to concentrate on one or two countries, perhaps China or Japan. Either of them would be more than enough for one report. The bare information I have found (on the web page `http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm` for example) is sketchy but interesting. See what you can develop, please.

I suspect that the laws and the practices of these governments might not be totally the same: that is, what the governments declare is legal and what they are willing to tolerate may be different. But I may be wrong. I would like you to concentrate on presenting policies and laws which might seem strange or restrictive to U.S. people but which your "country" insists on. You might consider the following supporting positions:

- Our traditions are not the same as those of Western Europe and North America, and we will not abandon our own culture and history.
- We have special (perhaps temporary!) needs for controlling security in communications, since we have been threatened historically by our neighbors, country X and country Y and ...
- Our resources have been exploited miserably by international corporations and we must be able to monitor communications to prevent possible future exploitation.
- Residents of our country must be willing to sacrifice some privacy so that our future will be better.

In your oral rebuttal

Of course be prepared to defend "your" country's positions. Assert that you are correct, distort history and economics judiciously if necessary to support your wishes, claim sovereign immunity, etc. Have a few facts ready if you absolutely need them!