Dr. R. Beezer — Math 133
Practicum #9 — Fall 2003
Anonymous Remailers

Sometimes we don't even want somebody to know we are talking to somebody else, even if the messages are securely encrypted. Or the volume of communication between us may suddenly spike up, alerting an adversary that we are planning something.

Or we might want to send a message to somebody anonymously. Perhaps we wish to alert the news media of abusive practices by the secret police, without fear of being revealed as the source of the alert.

So we are going to use "anonymous remailers" to disguise the origin and destination of our messages and frustrate Eve. Or we could use these remailers to disguise our identity as the author of a message.

Procedure

1. I will be sending you an email, routed through a "Type II Mixmaster" remailer. This is a sophisticated collection of servers that initially encrypts your message using the public key of another server, and then chops your message up into bite-size pieces for emailing to the next server. This receiving server will reassemble the message, encrypt it for another server using that server's public-key, then chop it up into identical pieces for emailing to that server. All told, my message will pass through three or four servers, but in transit, it will be PGP-encrypted, and it will always travel in pieces of identical sizes (both my message, and those of everybody else using this system) after being busted up for each trip. It will be very hard for Eve to track my message to you after all this encrypting and chopping/reassembling. She will be really frustrated.

2. How will I prepare my message? I don't trust the remailer operators, so I will encrypt my message to you with your public key, so only you can read it. That way, the remailers can't read my message to you.

3. If its anonymous, how do you know the message is from me? I'll sign it, of course. You should never trust the sender's name on an unsigned message, but you should be doubly suspicious of the alleged sender of an unsigned message sent via a remailer.

4. You do not need to do anything with the message I send you, its just for demonstration purposes.

5. Now you should send your own message to me via a remailer. We'll be using the slightly less-advanced "Type I CypherPunk" system since with PGP and WebMail (or your mail client) we have all the software we need.

6. First you need a public key for a remailer server. Where do you get that? Check the course WWW page. The `noreply.org` site's Thesauraus is a good source of information. Pick a remailer, perhaps based on its "uptime" (how often it is in service), and its latency (how long it takes to relay a message). Send an email to the server's email address by formulating a message with the **subject line** filled in with `remailer-key`. Don't put anything in the body of the message.

7. You should get a reply quite quickly containing several public PGP keys for the server. Ignore any "mix" keys that you get. Add the newest PGP key to your public keyring.

8. Now you can begin formulating a message to me for remailing. Find a pithy quote to send me. Sign it using your private key (I won't believe its from you otherwise), and encrypt it using my public key so its for my eyes only. Paste it into Notepad, or an email window and add the following to the start of the message, **before** the stuff that begins the PGP part of the message:

   ```
   ::
   Anon-To: beezer@ups.edu
   Latent-Time: +0:30r

   ##
   Math 133, Practicum #9
   ```

   The spacing, blank lines, etc. must all be just right. Two colons, new line, "Anon-To:<some email address>", "Latent-Time: +h:mmr", blank line, two pound symbols, then the subject line of the message I'll eventually see, followed by a blank line. After this should come all your PGP-encrypted stuff. It should be clear how to send an anonymous message to somebody else.

9. The "Latent-Time" instruction will delay your message for a random time, up to that specified in hours and minutes. Remove the "r" and it gets delayed for exactly as long as you specify. You wouldn't want Eve to see your message go into the server, and almost immediately come right back out, now would you? However, this entire line is optional, and can be omitted.

10. Right now, this message says exactly who you are sending it to. That's clearly unsatisfactory if we want to frustrate Eve! Encrypt the whole thing, only now using the public key of the server you will be sending the message to (that's the newly-obtained key you got in response to your email asking for it). The server will then decrypt it, and then read the instructions about who the message goes to, how long to delay it, and what the subject line should be.

11. Now you have one big encrypted message. Insert the following at the top:

    ```
    ::
    Encrypted: PGP
    ```

    Again, get the format just right on this one, and note that there is a blank line separating this stuff from the PGP part of your message. This will tell the server that we are doing Type I style remailing. (Don't encypt this again or the server won't know what to do with it!)

12. Ready? Send this to the server (not me). This is the same email address you used to get the remailer key a little bit ago.

13. Don't worry about doing the proof-of-posting timestamp routine on this one!

Grading
Full credit once I receive a message, signed by you, that comes to me through a remailer anonymously.

Notes

1. Hopefully the remailers are all legitimate, and not "honey-pots" setup by the secret police. Presumably the remailers keep little, or no, information about your message. But, just in case, we encrypted our very original message using the recipient's public key, so the content of the message will be safe in any event.

2. if you replace the "Anon-To:" instruction with "Null:" the remailer will just discard the message. Sending out a few spurious messages like this will **really** frustrate Eve.

3. For extra security, you can chain remailers. Instead of having the remailer send the message to me, have it send the message to a second remailer. However, you have to be very careful about setting this up, the message the first remailer sends to the second should have the right instructions for the second remailer, and be encrypted with the correct public key for that server. This is sort of like putting a message in an envelope with an address on the outside, then putting that into another envelope and addressing that one, and...

4. Many remailers will automatically route your message through one extra remailer. So for the price of one, you'll likely get two.

5. Note that remailers serve two functions — they allow you to disguise the origin and destination of an electronic communication. They can also be used to hide the identity of the sender, so they can be used by "whistle-blowers." However, you should always question the motives of the sender of a truly anonymous email. In this exercise, I have asked you to sign your messages, so I know they are from you.

6. We could have the final remailer in the chain send the message to Stamper for timestamping. We would just have to make sure this message was of the right form for Stamper's server.

7. I've seen what we are doing referred to as "rolling your own," since there are specialized programs that will concoct your message in just the right form for chaining through several remailers once it is configured properly.

8. As always, check out the links on the course WWW page. There's a lot of good stuff there.