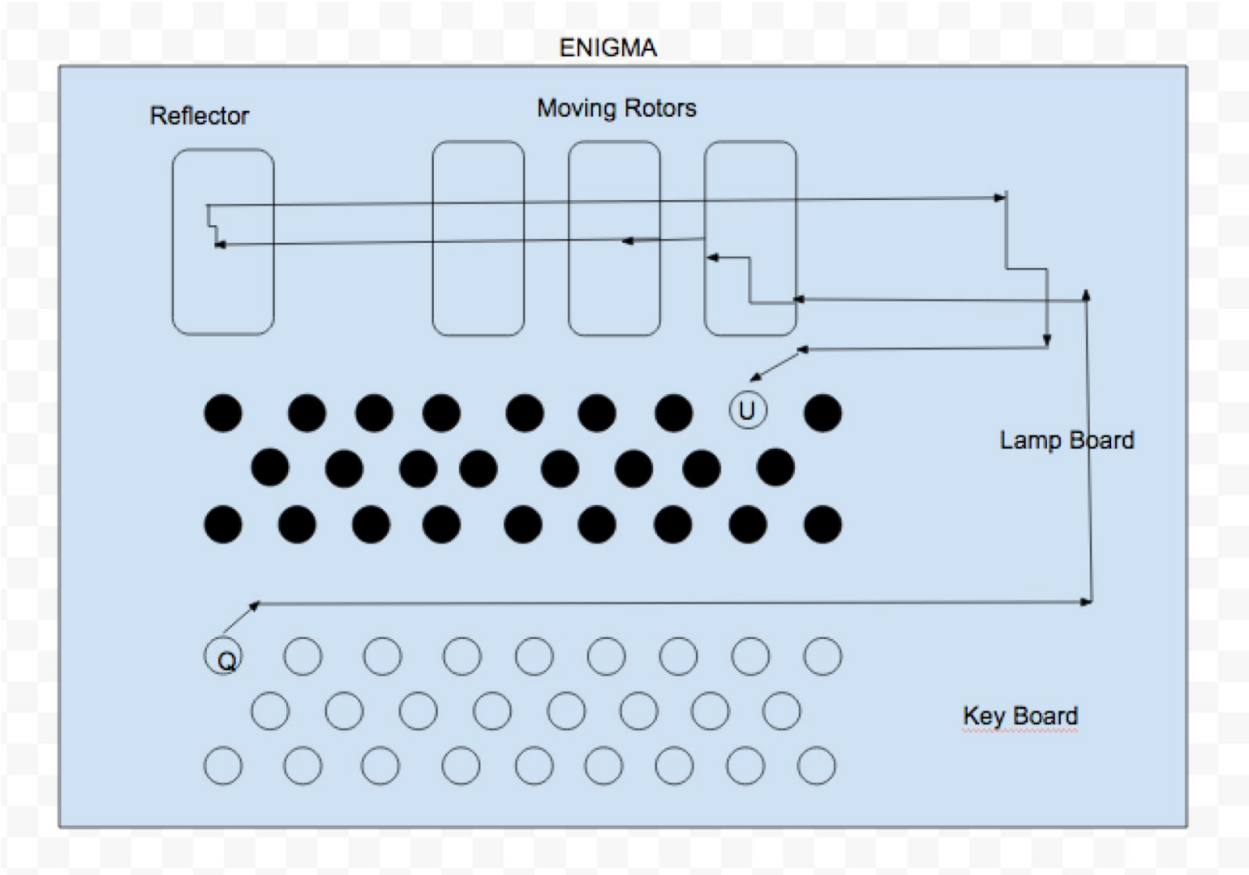
Paul Diaz
CS 166
Homework 1

9.a



Enigma consists of a keyboard, lamp board, three moving rotors, and a reflector. When a user types in keys in the keyboard, an electrical current runs through the three moving rotors and encrypted the key every time it exists a rotor. The encrypted key runs through the reflector, then back to the rotors - the appropriate key encrypted outputted by the first/last rotor will light up in the lamp board. As the current runs through the first moving rotor, it will rotate one full revolution before the current runs through the next rotor. The key entered by the user gets remapped to another letter If a key has a relation to another key. Note that each rotor has one to one mapping of letters; and since the rotors rotate every time a user presses a key, the mapping of the rotors changes. In order to decrypt the message encrypted, the receiver must know which rotors were used and the initial settings of the rotors. The receiver must set the machine the same way the sender did. This way, the receiver will have an output the same as the sender's original message.

9.b Hut 8 was led by Alan Turing at Bletchley Park in the U.K.; they were able to crack the Enigma code during World War II. For this reason, the British military and allies were able to

read all the German communication, specifically German military movements and routes including where (places) do they plan all their attacks. British military and allies subsequently prevented all German's attacks from winning; then German forces eventually were defeated.

11.a Yes, it is possible to authenticate based on something that I am; biometrics. Examples are fingerprints and eye scan/iris recognition. Fingerprint authentication is currently used by the recent iPhone and iPod technologies/devices instead of entering passwords to unlock and update the device and/or install a program in the system. Also, when I applied for my green card last year, fingerprinting is one of the requirements. Whenever I get back here in the states from other country, immigration officers will scan your fingerprints to map and pull out your file from their database.

11.b Yes, it is possible to authenticate based on something that I possess. Although, this material, a smart card for example, must be with me all the time, it solves the problem of forgetting something bases on what I know (passwords). Another example is the smart card that I have in my current job. It serves as an identification and access pass to open doors and some files in the computer system that other people may or may not access at my workplace.

11.c An example of two-factor authentication, also known as two step verification, is paying something from the stores using a debit card. When I purchase books, say in SJSU bookstore, with my debit card, I need to swipe my debit card in the machine (debit card is something that I possess), as the machine reads the card, it will prompt to enter the password (something that I know). The two authentication factors used are something that I possess (debit card) and something that I know (password).

13.a In terms of convenience, considering no steps required or needed to be done in order to finish and run the whole protocol, I think that it is convenient for both Alice and Bob. However, in terms of security, I think that this scenario is not good for them. I appreciate the brief warning of the computer stating that the protocol fails, but I don't see the purpose of it if Alice and Bob are not able to intervene or do something about it in order to prevent the protocol from failing at least prevent it from executing the failure – for security purposes. I'd say it is convenient but most definitely not secure.

13.b This scenario is a little better than in scenario 13.a, in terms of security. This is because the protocol prompts and informs the user that the protocol fails. I like the idea of warnings; however, the choices given to Alice where she wants to continue or not is a bit stupid. If this scenario were given to a novice/beginner user, where most of them don't really read warnings and accidentally click on something that they are not supposed to. Alice's scenario, for example could lead to crash and possibly risking her security. I'd say this scenario is less convenient and somewhat secure.

13.c This scenario provides a really good security because it forces the transaction to terminate when protocol fails; this is one way of preventing logical anomalies from happening, especially if

the transaction you're trying to do is altering data values (bank, database etc.). The downside of this scenario is not letting Alice and Bob complete the transaction. On the bright side, notification will be shown to Alice and Bob, this way they will know what went wrong. So I'd say this scenario is most secure but it is inconvenient.

13.d In terms of convenience, I think that this scenario is worse than 13.c, because if protocol fails, the transaction just terminates without any notification. In 13.c, a notification is shown to the user. This is recommended; this way, we will know what to do next time. In terms of security, same as in 13.c, good security, because it forces the transaction to terminate when protocol fails.

15.a Besides that fact that buggy software is absolutely annoying, it is also a security issue in so many levels because malicious users could derive benefit from the flaws, (brought by being buggy) which could compromise Alice and Bob's sensitive information.

15.b Trudy loves buggy software, especially is she gets familiarized and understands the software's loopholes. Trudy can easily acquire access to say, SJSU database, and maybe alter her grades or financial activities in the system.

15.c As soon as Trudy successfully installed bugs in a computer, she can easily take control over a computer and break in and compromise the security of the system. Trudy can even lurk in a computer for a while and *sniff* user's activities; like recording the websites that the user visits, records credit card information when the user purchasing something online, etc.

Article Summaries

- Keystroke sniffer (Links to an external site.) at http://hackaday.com/2015/01/14/keystroke-sniffer-hides-as-a-wall-wart-is-scary/

  This video article talks about keystroke sniffer, an Aduino device that camouflaged as functioning USB wall charger that wirelessly sniffs, decrypts, and logs all keys pressed by a user. It also reports and logs all keystrokes from any Microsoft wireless keyboard (with this device connected), then logs all keystrokes and store them online and/or inside the device. This article emphasizes that the scary thing about this technology is not the device itself, but it's how weak the encryption of it for Microsoft keyboards, and ultimately compromise user's security.

- EBay asks 145 million users to change passwords after cyber attack (Links to an external site.) at http://www.reuters.com/article/2014/05/21/us-ebay-password-idUSBREA4K0B420140521.

The article talks about a cyber-attack on eBay happened between the month of February and March 2013. EBay's customer database was compromised and found that hackers stole eBay's customer's email addresses, encrypted passwords, birth dates, mailing addresses, and other sensitive information. EBay's customers were advised, about 145 million online users, to change their passwords. Representatives of eBay conducted an investigation on this breach in case of fraud cases. Thankfully, as of June 17, 2013 (date publication of the article), there was no sign of fraud.

- Regin (Links to an external site.) at http://money.cnn.com/2014/11/23/technology/security/regin-malware-symantec/index.html (Links to an external site.).

  This CNN tech article reports about a cybersecurity threat called Regin. This Malware is not the typical program that steals information in our computers/devices – stealing credit card information and/or social security number. It is some type of spying tool that that was found to be lurking in many computers around the world for about nine years now. According to Symantec, a cybersecurity company that created Norton Virus, Regin was found in many computers in at least 10 countries – heavily concentrated in Russia and Saudi Arabia. Symantec analyst Vikram Thakur explained that Regin is trying to "gain intelligence, not intellectual property." Symantec also said and found that Regin malware has a capability to conceal itself and provide a high level of security protection when Semantic attempted to reveal this malware. It also mentioned in the article that Regin is very similar to the Stuxnet worm – well-known virus that believed to be designed by the United States and used to hack Iranian nuclear program.

- https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/karapanos (Links to an external site.)

  This video article was taken at the 24th USENIX Security Symposium took place on August 12-15, 2015 in Washington, D.C. The video starts off by talking about different authentication. Web authentication typically uses passwords as a mean of authentication. The reason why people are not fond of using two factor authentication is its inconvenience —that extra step that users must do, like entering verification code sent to their phone or alternative email address. This symposium proposes a technology called Sound-Proof, a two factor mechanism, where the second factor authentication (verification code that typically sent to phone) is not *really* required anymore. The second factor authentication is actually done behind the scene/virtually – it is the "proximity of user's phone to the device being used to login." This is done by making the computer and phone communicate with each other using the "ambient noise recorded by their microphones." Prototypes have already been built compatible with iOS and Android devices. This technology provides a great reliability function because it has a robust discriminant device that determines the proximity between two devices.