Research Manual

PASSWORD MANAGER

(C00246523) - JASON DARLEY

Contents

Project brief

Design:

For my password manager I want to use java to code 2 programmes:1 will be a password generator with a gui that will have options on it to choose what you want the length by adjusting a slidebar to be a certain length and it must contain symbols/caps/lowercase/numbers there will also be a message on it that gives some tips about what a strong password is.

For the password manager I want to store the passwords in a mysql table and have the passwords be protected by encrypting the passwords using aes. For the aes each user will have their own unique key which gets created for the user when they make their accounts. The key will be created using a random generator.

I also want to have a main menu gui with a menubar that provides easy navigation to the users to find whichever page they want like the strength tester, generator, view passwords etc.

When you have the main menu open and click one of the buttons to open a page like the generator or store a new password. I want the main menu to stay open so the user can access the other options easily instead of having to go back and not being able to have access to the store passwords page and have the generator open at the same time.

I also want to try and make it so when you do enter a password for the file I want it to show as ***** instead of showing the plaintext password by using password fields in java instead of text fields, and I also want to make the generator only generate strong passwords so they can ensure security when using the passwords for their personal accounts on different sites and apps.

Encryption:

I want to encrypt the contents of the text file using aes to make the passwords as secure as possible so in the case of a breach the passwords will be extremely hard to crack as each user will have their own key to encrypt and decrypt the passwords.

AES

The Advanced Encryption Standard or AES is a symmetric cryptographic encryption algorithm established by the United states National Institute of Standards and Technology (also known as NIST) in 2001. The advanced encryption standard is widely used today due to how strong the encryption method is compared to others like DES and triple DES but AES is harder to implement. Symmetric cryptography is when the same key is ued for encryption and decryption while asymmetric cryptography is when you have a public and private key for the encryption and decryption processes. AES is considered to be one of if not the best and most secure encryption algorithms to this day.

AES is a block cipher which is a method of encrypting data in blocks to make the ciphertext using a cryptographic key and algorithm. AES uses a cryptographic key that can be a size of 128, 192 or 256 bits and it will encrypt data in blocks of 128 bits each which means it takes 128 bits as input and also outputs 128 bits of ciphertext. AES uses substitution permutation which means it performs using a series of linked operations using shuffling and replacing of the input data. AES works by operating on bytes instead of operating on bits of data and processes 16 bytes or 128 bits of data at a time. AES also uses a round system which is how many times the process is executed and the amount of rounds performed depends on the key size, a 128 bit key will have 10 rounds, a 192 bit key will have 12 rounds and a 256 bit key will have 14 rounds of operation. For AES each round consists of 4 steps and these steps are

SubBytes, ShiftRows, MixColumns, and Add Round Key and during the final round of the encryption process mix columns is not used. SubBytes performs the substitution while the shift rows and mix columns perform the permutations. For the SubBytes step each byte gets substituted by another byte, its done by using a lookup table which is called an s-box, the byte will never get substituted by itself or by another byte which is a compliment of the current byte. For the shift rows step each row of a 4 x 4 matrix which makes the 16 bytes is shifted a certain amount of times, the first row does not get shifted, the second row is shifted once to the left, the third row is shifted two times to the left and the fourth row is shifted 3 times to the left which looks like this:

[b0 | b1 | b2 | b3] [b0 | b1 | b2 | b3]

| b4 | b5 | b6 | b7 | -> | b5 | b6 | b7 | b4 |

| b8 | b9 | b10 | b11 | | b10 | b11 | b8 | b9 |

[b12 | b13 | b14 | b15] [b15 | b12 | b13 | b14]

For the Mix Columns step this is a matrix multiplication so each column gets multiplied by a specific matrix which will change the position of each byte in the column, this gets skipped in the final round.

The add round keys step is the result output of the previous stage and is xor-ed with the corresponding round key. After the 128 bits of encrypted data is outputted this step is repeated until every piece of data is encrypted with this process.

To decrypt AES you do the encryption process in reverse so you do add round key first then inverse mix columns then shift rows and finally inverse sub bytes.

AES has 5 different modes of operation:

1: electronic code book mode (ecb)

2: Cipher block chaining mode (CBC)

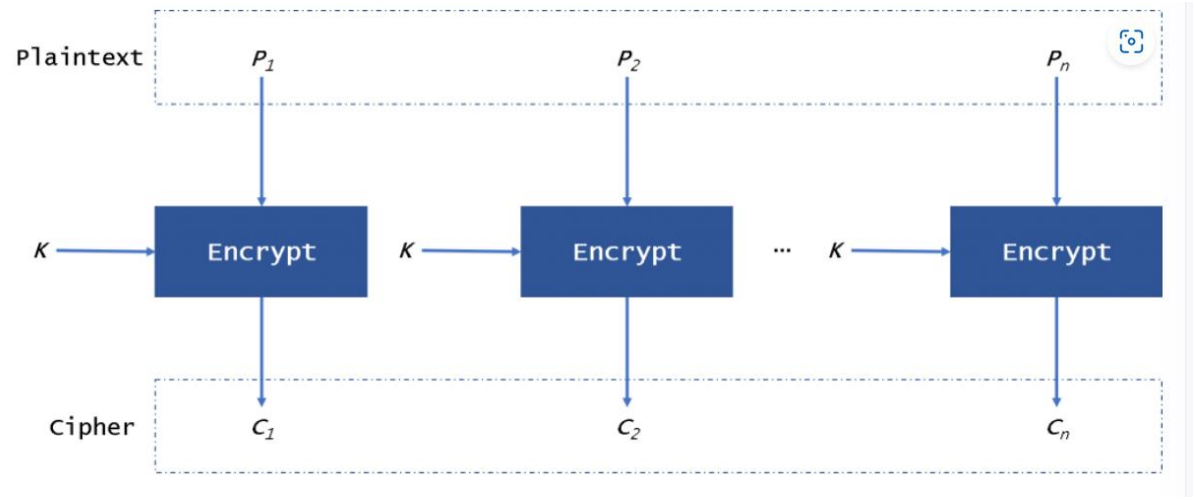
3: Cipher feedback mode (CFB)

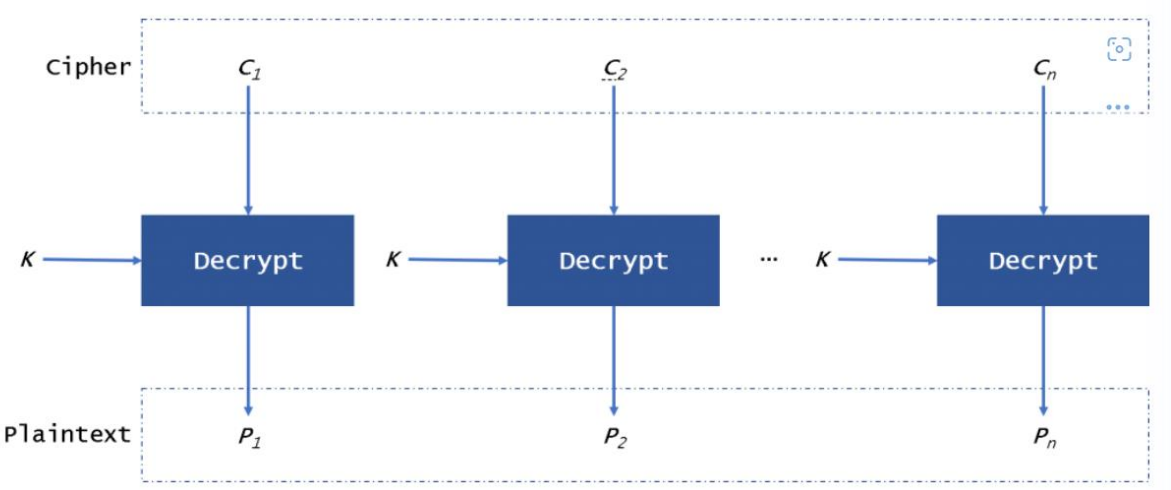
4: output feedback mode (OFB)

5: Counter mode (CTR)

ECB Mode

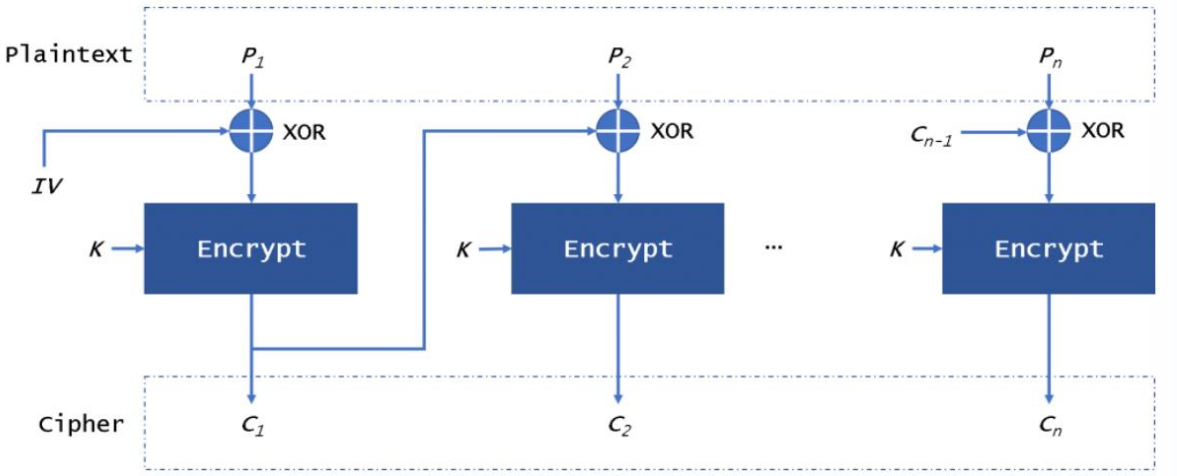
Ecb mode is the simplest version of aes and is not recommended as ecb pads the data when encrypting but if you encrypt a piece of plaintext and then encrypt a copy of that plaintext they will become the same ciphertext and this is not secure as there are sites with databases of what the plaintext will become when using ecb mode so hackers can easily find the plaintext of your data by using these sites.

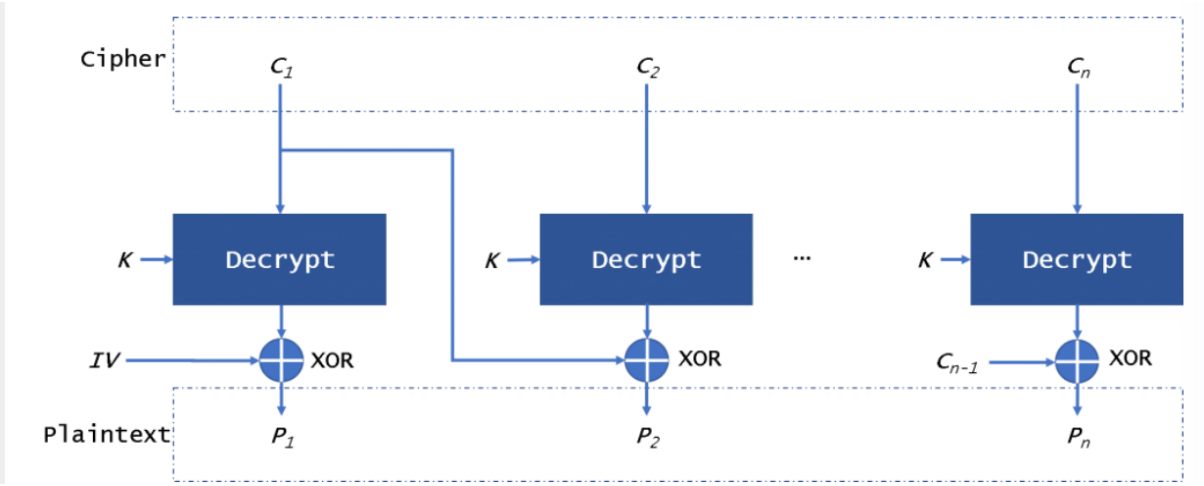




CBC Mode

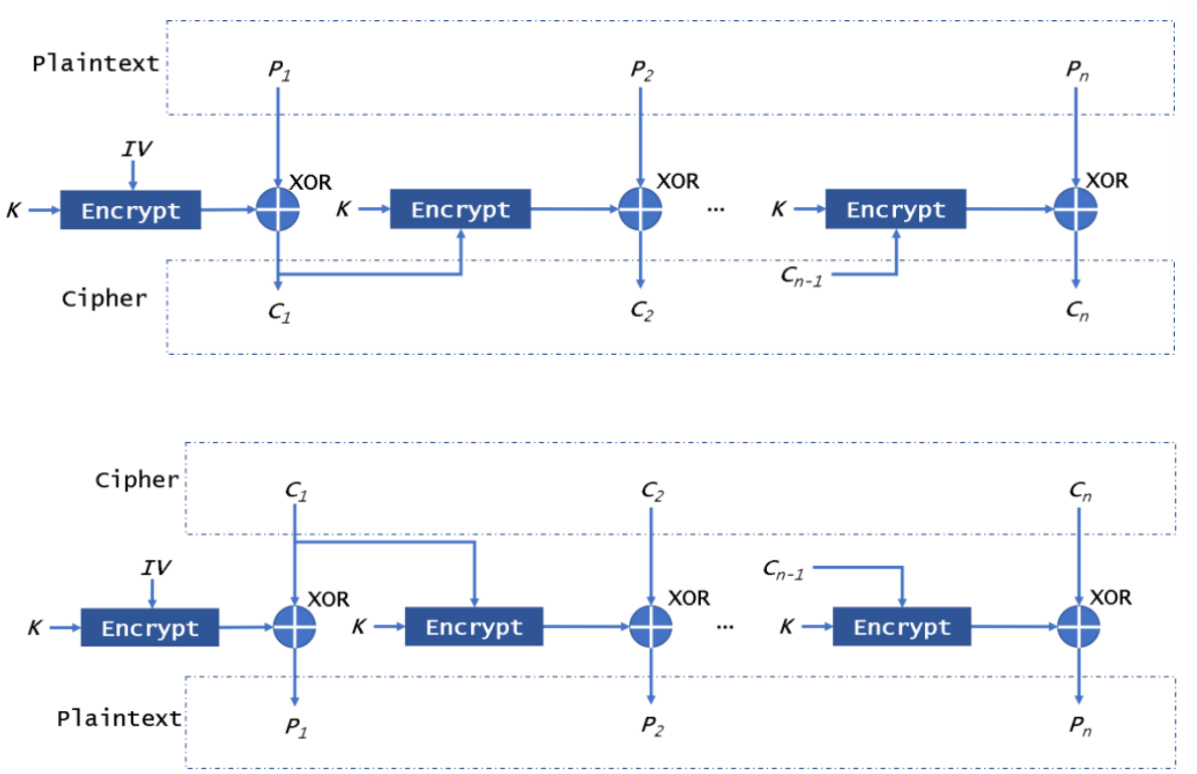
Cbc mode divides the plaintext into blocks and pads the data, then the plaintext block will be xor-ed with an initialization vector which is a random number and then will encrypt the result to the ciphertext block, in the next block the ciphertext block that was just made will be used to xor the next plaintext block and this process will carry out until all the data is encrypted. In this mode when we encrypt the same plaintext data it will be different as the plaintext is being xor-ed by a new piece of data every round which makes it way more secure than ecb mode.





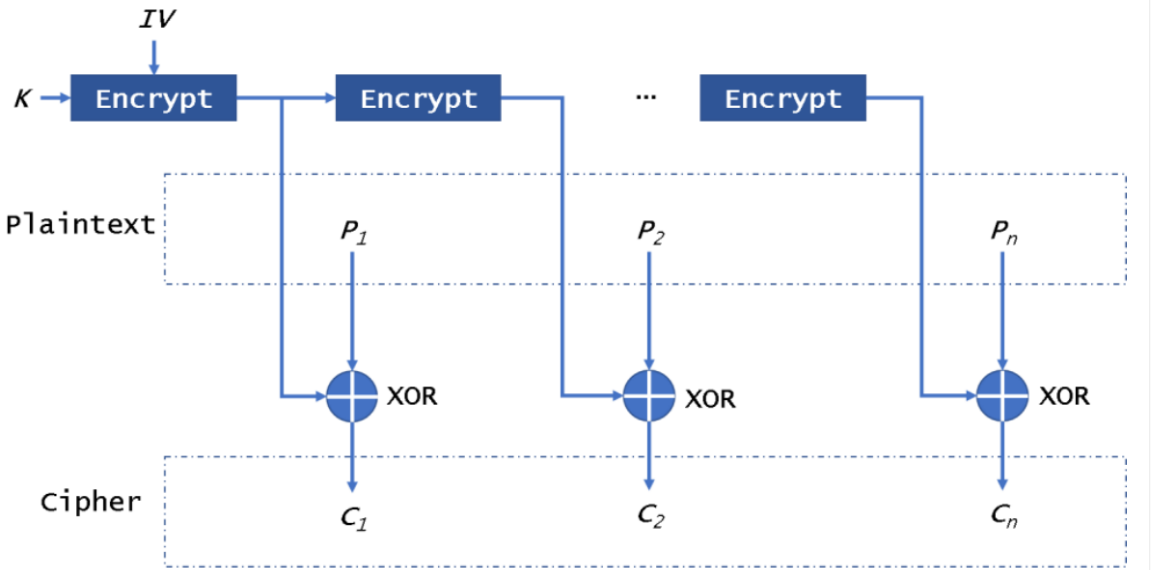
CFB Mode

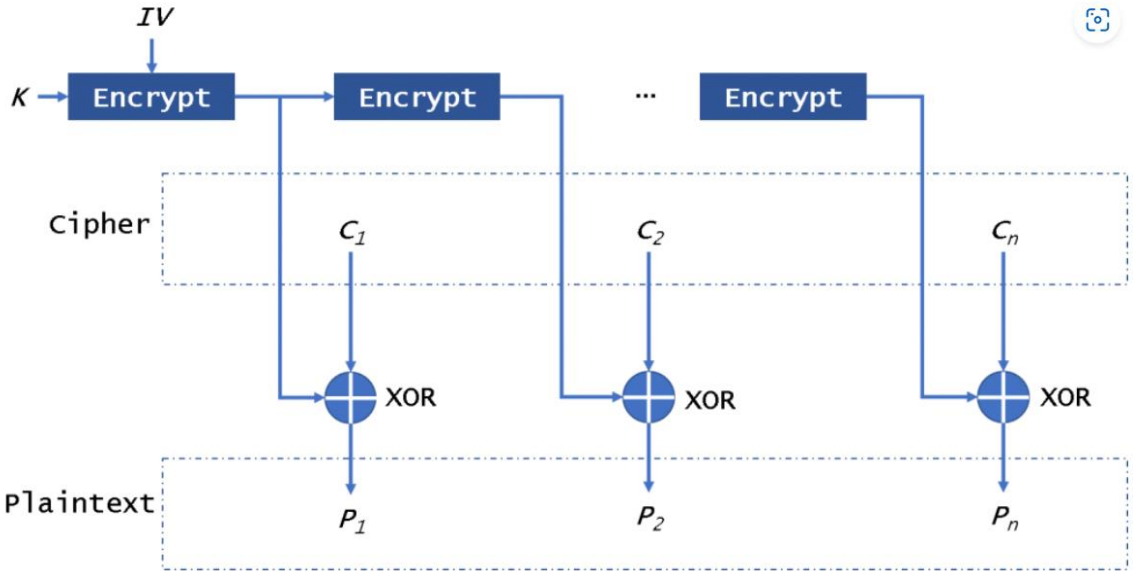
CFB mode will encrypt the iv then xor with the plaintext block to get the ciphertext and then will encrypt the encryption result to xor the plaintext block. This mode does not need to pad data This mode can be attacked by a replay attack, if you use the ciphertext to replace the new ciphertext the user will get the wrong data without knowing.



OFB Mode

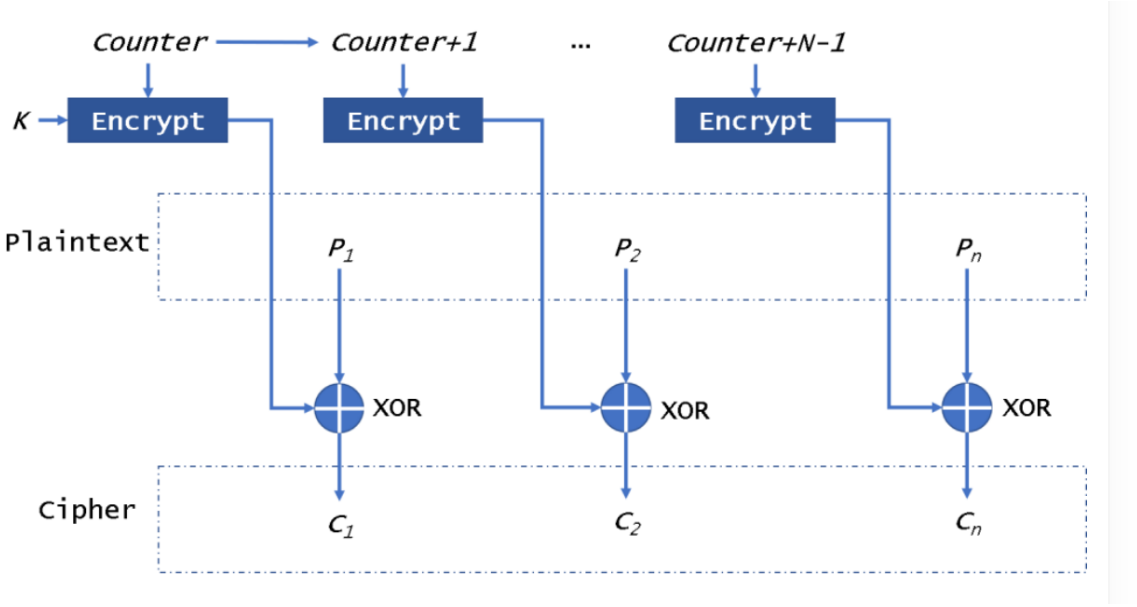
Ofb mode will encrypt the initialization vector in the first time and encrypt the result, then it will use the encryption result to xor the plaintext to get the ciphertext.

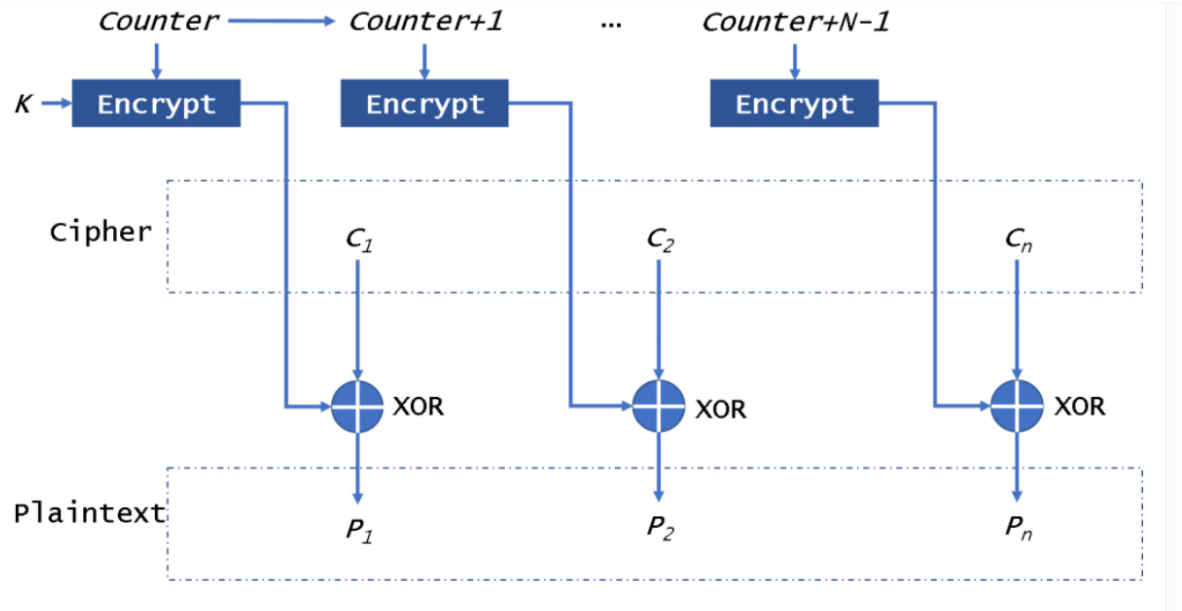

IV
K
Encrypt
Encrypt
...
Encrypt
Plaintext
P_1
P_2
P_n
XOR
XOR
XOR
Cipher
C_1
C_2
C_n


IV
K
Encrypt
Encrypt
...
Encrypt
Cipher
C_1
C_2
C_n
XOR
XOR
XOR
Plaintext
P_1
P_2
P_n

CTR Mode

Ctr mode has the same size as the used block, the xor operation with the block of plaintext is done on the output block from the encryptor, all encryption blocks use the same encryption key.

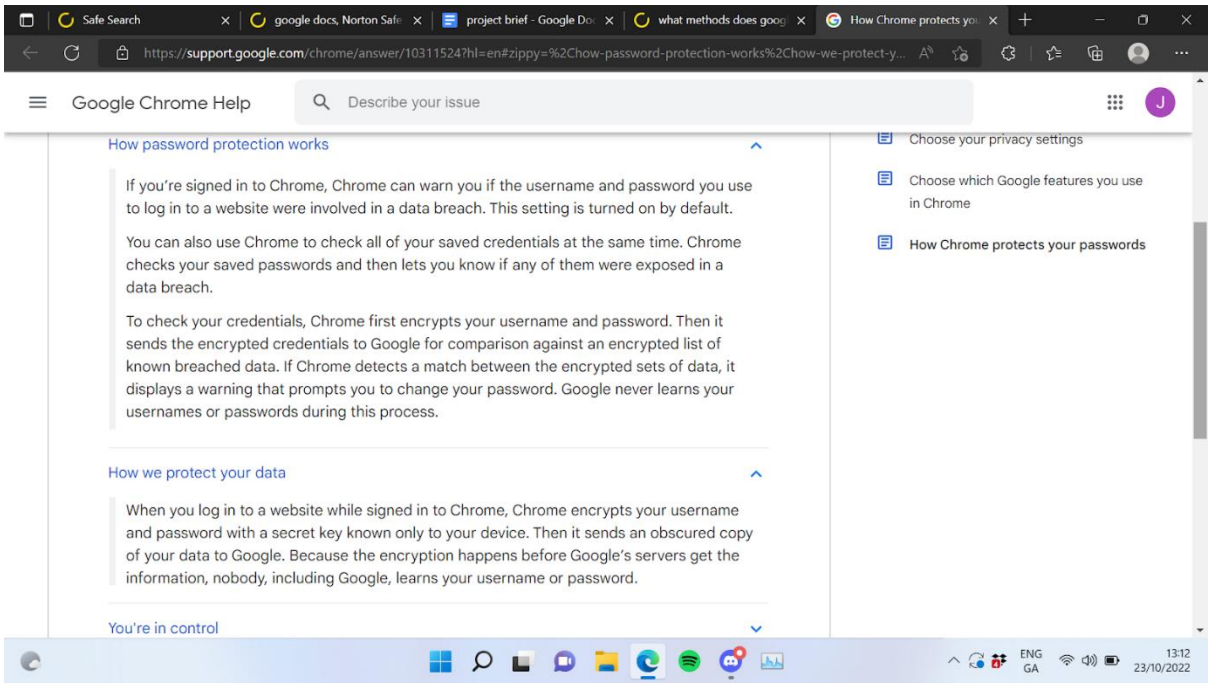




Reason for Use

I want this to be used over different password managers as some don't have generators and some don't use as good of encryption so this password manager can guarantee good security and ease of use by having a simple yet useful and effective gui to give the user the best use out of it. I will also use this for personal use to keep my own information secure

How do other managers like google encrypt and store their passwords.:



For google password manager they state they encrypt the information before it reaches the servers but this can lead to a man in the middle attack who can take the request and change the information to whatever they want before it reaches the destination it also lets you use the same passwords as other accounts of yours if the

password hasnt been breached but if you do keep using the same password if 1 site gets hacked then all of your passwords are breached as their the same.

For microsoft edges password manager they use aes to encrypt the passwords but theres no mention of them using salting hashing or peppering so this can lead to somewhat easy breaches if the attacker gains access to the encrypted password as they can just enter the information into a site that can instantly decrypt aes since theres no signs of hashes, salts or peppers.

Both google and edge use an extension that will automatically paste the credentials into the sites which is a bad security measure as if somebody gains access to either your email account and use that email on google or edge they can go to any site you use and can instantly login and if the attacker even just gets access to the users device and doesnt need to steal the email credentials they can go onto the sites and login as the credentials instantly get pasted in and then the attacker can do whatever they want with the account.

Check if other managers have a training section describing why certain measures are good and safe.: from what i could find theres no training included in other managers just separate training about password management on training sites like infosec theres no training included in any password managers i could find.

Research password strength testers.: for password strength testers it considers a password to be very strong if it included upper,lowercase characters numbers and special characters so since that will be the default for the generator to use all of those the passwords will be strong.

Look up pros and cons of random passwords and password manager.: from what i could find the only con of random passwords where that there easy to forget but if you use a password manager thats secure you dont have to worry about forgetting the passwords and the pros are that its highly secure as hackers cant use dictionary attacks against it and you cant be social engineered for your passwords as they will all be different and you wont be able to remember them all as easy as you will with basic passwords.

Hashing

Hashing is when you change the inputted text into a random string of a certain length depending on which type of hashing algorithm you decide to use. Hashing is different to encryption as encryption is a 2 way process where you can change text into a random string of the same size and can also change that random string back into its original text using a unique key, there are multiple ways of encrypting such as Caesar cipher, vigener and so on while hashing is a 1 way method which will take a piece of text and change the text into numbers and letters like encryption but it will also make the text longer to reach a certain length so it cant be deciphered only compared. Hashing will always have a certain text using the same hashing algorithm be the same value so if I hash the word hello using sha(256) hello will become 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824 but if

someone gets this hash value they cant change it back to hello but they can use software that compares hashed words to the hash and there will be libraries that will find that hello is equal to 2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824 every time as it doesn't change the outcome each time its inputted as it needs them to be the same in order to compare the hash values. For hashing if you store a password, it will be hashed using the algorithm and when asked for your password again to login it will hash your input and compare the hash of your input to the hash that's stored of your password if they are the same hash then it will log you in as your password matches. Since an attacker can just run your hash into software that will find which word will hash into the hash, they stole they can find your password easily so in order to secure the hash you must use salting and peppering.

Salting and peppering

Salting and peppering is when you add a random string of characters to a string/text before hashing a password. By adding the salt to the password before its hashed it will cause the hash to be completely different than if there was no salt which makes passwords more secure as attackers are able to find the original string of hashes through trial and error so by adding this random string to the text before hashing it makes the hash completely unique and a lot harder to find the original text from the hash. Peppering is the same as salting, but you should store the pepper in a different location than the salt as if an attacker gets access to one they won't have the other and the password will remain safe while if there both in the same database/location and the attacker gains access to them the passwords are then insecure and can easily be reversed using software to find the outcome of hash values.

Where do you store peppers.: peppers are stored in a separate database from the salt and encrypted password/information in case theres a breach of 1 database the hacker wont get everything they need to decrypt the password/information. Pepper are also used in order to tell if a database has been breached, the pepper should always be the same for a table in the database and each table should have a

different pepper so if theres a breach you can tell which pepper was assigned to the breached information and therefore tell which table has been breached so it makes it easier to do incident response and implement more security measures as a table might be missing techniques from other tables/databases.

Sha 256

Sha256(secure hashing algorithm 256) is a cryptographic one way function used for message,file, and data integrity verification. It uses a 256 bit key to make a piece of data unrecognisable and make it a fixed length. Its part of the sha-2 family which contains sha-224, and sha-256. Its called sha 256 as the hash is 256 bits long. Sha256 is the industry standard hashing algorithm as it's the most secure and hasn't been broken. Sha256 was designed by the national security agency(nsa). The US government patented the algorithm but released it as a royalty free license for everybody to use for free. Sha256 uses 64 rounds and a round is a set of functions repeatedly carried out in the algorithm to make the data unrecognizable. It also uses shifts which are divided into 8 segments of 32 bits each and then the 8 segments are shifted randomly to make the data unrecognizable. Additive constants are values added to the blocks, there are 64 constants used to add to blocks and the numbers are the cube roots of the first 64 prime numbers. Sha 256 is used for protecting the data integrity for when communicating online and assume the reply is coming from a trusted/known person, sha 256 will ensure that both parties can verify that the other person is who they think they are and can confirm if its them. The recipient device creates a hash of the original message to compare it to the hash of the message sent by the sender and if both of the hashes are the same then the message hasn't been tampered with in transit. Its also used for verifying digital signatures, digital signatures are a way of signing digital documents, code, or software that's verifiable by the recipient user. This is used to verify if the item was tampered with. The digital signatures are created by applying a hash to the file and using and encryption algorithm to encrypt it via public and private keys. The private key is used when the signature owner signs the document while the public key is used by the recipient to

decrypt the message on their end. sha 256 is one of the most reliable algorithms for authentication and message integrity verification. Sha256 is used for: 1.ssl/tls to maintain data integrity and confidentiality while its in transit.

2.ssh – creates a secure channel between two devices for data transfer.

3.ipsec – is a collection of protocols designed to secure data transfer across different ip networks.

4.pgp – is an encryption algorithm used to sign encrypt and decrypt emails files directories and a disk partition.

5.s/mime is an algorithm to secure the integrity and confidentiality of emails.

6 – blockchain – in a blockchain preceding hash values are used to calculate the hash value of the current block.

In order to crack sha 256 you need basically unlimited resources and time so sha 256 is secure as it hasn't been cracked yet which is why bitcoin uses this algorithm. And tls certificates also use sha 256 to validate the integrity of the certificates.

There are 2 essential stages of the sha 256 algorithm

1. Preprocessing – this is where the message gets padded and broken down into smaller blocks and initialisation values are set.
2. Hash computation – this involves a series of operations that result in a series of hash values. The 256 bit hash digest is the result of these various hash values.

Multi Factor Authentication

Multi Factor Authentication or MFA is a security technique that requires a user to confirm their login attempt by receiving a link or usually a code to a personal device or their email, they then have to enter the code into the site or app to gain access. I plan on using java to send an email with a 6-digit code when attempting to login or change the accounts

password to ensure it is the user trying to perform these actions and not a threat actor. The code will be randomly generated and stored in a table on the MySQL database and sent to the user. The user will then enter the code and if it matches what's stored in the table then they will be granted access or will be allowed to change their password for their account on the password manager.

Reason for a Password Generator

A password generator should be used for making passwords as they use randomisation which prevents social engineering from happening as your password wont be something like the name of your favourite sports team, by using randomness it also helps against brute force attacks mainly dictionary attacks as if you use a regular word as your password there are scripts that will test every word in the dictionary so using normal words is insecure because of brute force attacks and the best way to prevent these attacks is by having a password that is essentially unguessable and the best way for it to be unguessable is to make it random.

Notepad vs storing in database

For accessing the information stored I was thinking of either having it be pulled and displayed from a database to the user on the gui or have the information be stored and have the ability to edit the information on a text file from a notepad. With the notepad it will provide more security as a user can store the file in a password protected folder and in an attacker would have to gain access to the users device in order to access the file if they can even find it as the user can hide the file while all an attacker has to do with the database option is breach the database and since the information will be encrypted the attacker can decrypt the information with certain software a lot easier than gaining access to the users device and finding the file and accessing it if its in a password protected folder.

Java vs javascript why I chose java

I chose to do my project using either java or javascript with css and html but I chose to use java as it is harder to hack compared to a web page where attacks like sql injection, cross site scripting, path traversal attacks etc can be executed on the web pages and would require a lot of filtering and sanitization in order to make the password manager safe and protected while the java program doesn't have to worry about these attacks. Although you can make a nicer gui with javascript, css and html the security risks aren't worth it while the gui with java won't be as good it will still be good and have enough options to make the gui easy to use and nice on the eyes for the users while not having to worry about attacks as much as the javascript version.

MySQL

Mysql will be used to store the hashed, salted and peppered password to access the password file and decrypt the data when the file is opened. The password for the manager will be stored in the database and when the user enters their password it will use the same hashing algorithm and add the same salt and pepper that's stored in the database to compare the entered password and the stored password and if the passwords match it will allow access otherwise will present the user with a message saying incorrect password. (find a reference for this)

Limiting Login Attempts

I will be adding a counter to count the amount of failed login attempts and when there are 3 failed login attempts in a row it will close the programme. I want to implement this as it will prevent brute force attacks from occurring.

Prepared Statements

Prepared statements are used in order to prevent SQL injection. Prepared statements precompile code in order to separate the actual SQL injection attack from the data and when these are separated it can accept the code as a regular input and it won't execute the attack in the database. This helps with SQL injection as people can use SQL injection to change the logic of a login attempt to trick an application into thinking a failed login is successful and allowing access to the attacker.

Training

In a recent study 80% of business stated that within a 12-month period with regular cyber security training, employees were shown to go from a risk of 60%of getting hacked to a 10%risk of getting hacked, so I want to add free training with the password manager as other sites like infosec provide training, but you need to pay for it. The main topics of training I want to focus on are Phishing, Spear Phishing, Malware, Business email compromise, Ransomware, Social engineering, and password security. The training will provide enough knowledge for users to be able to identify and prevent these attacks from happening by teaching users how to spot a phishing link and tell the difference from a legit link and so on.

Phishing

In 2021 it was reported that 40% of attacks were phishing related. Phishing is when an attacker targets victims through email, telephone, or text message while the attacker poses as a legitimate person/site/company to lure victims into providing the attacker with sensitive information such as bank details, or passwords, the information is then used to gain access to accounts and can result in financial loss. Phishing attacks usually want the victim to act fast telling the victim they have a time limit to buy something that's on sale for instance, phishing email links will have multiple ways to identify them, if you hover over the link it will show the actual URL so if the actual URL and what you are hovering over don't match you know it's a phishing link, also it is very common for the links to have misspelled words where there's only a slight difference to a legit site say for instance one link is for "amazon" the legit site and the phishing link could have it spelt as "amaz0n" in order to trick people into clicking the link as they don't notice the spelling error. In cases where the

message being sent to you seems suspicious like a person you know is asking for money or information, you should contact that person in a different way than they contacted you so if you were sent an email, you should contact them through a phone call or text to confirm if they sent the email. In order to prevent phishing, you can apply spam filters that won't allow certain emails to come through depending on software used to send the email, the origin of the message and the appearance of the message, but spam filters can block legitimate emails so its not always accurate, but it will still do more good than harm.

Spear Phishing

Spear phishing is a phishing method that targets specific people or groups within a company. This method is used to cause network compromise, data loss, or financial loss. For Phishing attacks an attacker will mass send emails to random people while spear phishing attacks a certain person and involves prior research. The spear phishing attack will usually include an email and an attachment where the email will contain personal information of the victim such as their name and their position within the company which will increase the likelihood of success of the attack.

Malware

Malware or malicious software is a type of computer program that is made to infect a user's computer and cause harm in many ways. Malware can infect devices in ways such as trojans, spyware, viruses, worms and more. Its essential that users know how to identify and protect themselves and their devices from all forms of malware. Malware is most commonly sent through emails with messages saying "look at this cool video" and a link that will install the malware on the device, its important that a person knows when not to click on these links in order to stay safe but another way to stay safe from malware is by using antivirus software as these are solely made to identify and get rid of malware on a device and in some cases will tell you if its

malware before it even downloads and cancels any download attempts and can even tell if theres malware without any previous known reports of malware if the download intends to hide itself as this is a common sign of malware as it doesn't want to be found and can do as much damage as possible to a device.

Business email compromise

Business email compromise is a type of email cyber scam where an attacker targets a business to defraud the company. The FBI states there are 5 major types of the business email compromise scam:

1. CEO fraud – this is when an attacker positions themselves as the CEO of a company and will usually email an employee in the finance department asking for money to be transferred into the attackers account.
2. Account compromise – this is when an employee's email account is hacked and is used to request payments to vendors, the payments are then sent to the attacker's account.
3. False invoice scheme – this is when attackers commonly target foreign suppliers and act as if they are the supplier and requests payment transfers to their account.
4. Attorney impersonation – this is when the attacker impersonated a lawyer and targets lower-level employees as they won't have the knowledge to question the validity of the requests

5. Data theft – the attacker will normally target hr and attempt to retrieve sensitive information about employees in the company like the CEO and can then be used for CEO fraud.

   Business email compromises work from the attacker posing as someone in a company an employee will trust and then the attacker asks that employee for a transfer of money, or bank details. These are hard to detect because things like antivirus can't spot them as there's no malware being used, instead the attack relies on social engineering methods. In order for people to be able to spot these attacks they need to be thought the signs of the attack, the signs usually consist of high-level executives asking for unusual information, or they will request you don't mention the request to anyone else, there can be instances of grammar mistakes like broken English or they may format the date wrong like using the American format over European formats or vice versa. If the email seems suspicious the user should contact that person in a different way than how they were originally contacted, the attacker will usually send these requests during the busiest part of the day so you wont have as much time to think about if its legit or not so make sure to slow down and question the request.

Ransomware

Ransomware is a type of malware that will lock a user's data, or their device and the attacker will threaten to keep it locked, delete files or make personal data public unless the victim pays the attacker a ransom. In 2021 ransomware made up 21 percent of all cyber attacks and cost about 20 billion dollars to victims. There are different versions of ransomware such as double extorsions where the attacker requests a ransom to unlock the data and a ransom to prevent its theft, and there is the triple extorsion is the same as the double extorsion, but the attacker will also ask for a ransom to prevent the user from being the victim of a distributed denial of service attack by the hacker. Ransomware can be installed on a user's device in

multiple ways such as phishing emails, operating system and software vulnerabilities by targeting systems with out of date software or operating systems that haven't patched certain issues, credential theft where the attacker can buy a user's credentials from the dark web or brute force their credentials then login to a network and deploy the ransomware directly, attackers can also use trojan malware to install the ransomware onto the system, and finally there are drive by downloads which is when an attacker uses web sites to pass the ransomware onto a device without the users knowledge and they do this through web vulnerabilities found in the site. There are 3 stages to ransomware:

1. Reconnaissance – attackers scan the infected system to understand the device and network and see what files are of importance to attack.

2. Activation – the ransomware starts identifying and encrypting files, most ransomware attacks will use asymmetric encryption so the attacker will have a private key that can decrypt the data and since the victims doesn't know the private key they can't decrypt their data.

3. Ransom note – once the files have been encrypted or the device gets disabled the ransomware will alert the victim of the infection, the ransom note will contain information like instructions on how to pay the ransom in exchange for the private key and restoration of the data.

There are subcategories to ransomware as well and these are:

1. Leakware/doxware – This is ransomware that steals sensitive information and threatens to make it public.

2. Mobile ransomware – This includes all ransomware that affects mobile devices and is delivered through malicious apps or drive by downloads.

3. Wipers/destructive ransomware – This threatens to destroy the data if the ransom is not paid but there are versions of this that will destroy the data no matter what.

4. Scareware – This is when ransomware just tries to scare the victims into paying the ransom by posing as say the police demanding a fine be paid.

To protect yourself from ransomware and the key items that will be thought in this training is to:

1. Maintain backups of sensitive data regularly, ideally on separate hard drives or other devices disconnected from the network.
2. Apply updates constantly to prevent attacks through vulnerabilities of software or operating system.
3. Implement access policies like multi factor authentication so that ransomware cant access certain data.

Social engineering

Social engineering is when somebody tries to gain the trust of a person so that they lower their guard into taking unsafe actions like sharing personal information or clicking on web links or opening attachments that may be malicious. Attackers use this method in order to learn more about the company the user works for, like the name of their boss so they can then do business email compromise attacks, or they can install ransomware as the victims trust the attacker and will likely open a link from them which install malware or ransomware onto their device. In terms of security people are the weakest part of any security which is why 95 percent of attacks are caused by human error. Social engineering can allow an attacker to learn information about the physical building of the company like how many guards there are or what the security is like, and they may even be able to obtain a workers security badge if the company uses them. The best ways to prevent social engineering for a business is by using multi factor authentication so an attacker cant access devices or enter parts of the building without verification, anti-phishing defences should also be put in place that will prevent users from receiving phishing emails and there should be password policies so that the employees can't use a password that’s easy to guess like the name of their favourite football club as an attacker could easily learn this information. Attackers will use the following types of attacks in order to perform social engineering: phishing, watering hole attacks which

is when an attacker compromises a website that is frequently visited by a group in hopes to target a specific person in that group, business email compromise, physical social engineering, and usb baiting which is when an attacker install malware onto a usb and leaves them in strategic places hoping that someone from the target company or the target themselves will pick the usb up and plug it into the device so that the malware can install on the device. The training will consists on how to identify or prevent the social engineering from happening/when it happens and what to do when it does happen

References

What is the AES algorithm? (no date) *Educative*. Available at: https://www.educative.io/answers/what-is-the-aes-algorithm (Accessed: November 25, 2022).

Daniel, B. (2022) *What is AES encryption? [the definitive Q&A guide]*, *Trusted Computing Innovator*. Trenton Systems, Inc. Available at: https://www.trentonsystems.com/blog/aes-encryption-your-faqs-answered (Accessed: November 25, 2022).

Advanced encryption standard (AES) (2022) *GeeksforGeeks*. Available at: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/ (Accessed: November 25, 2022).

Shawn WangShawn Wang is a developer of PostgreSQL Database Core. He has been working in HighGo Software for about eight years.He did some work for Full Database encryption (no date) *The difference in five modes in the AES encryption algorithm*, *Highgo Software Inc.* Available at: https://www.highgo.ca/2019/08/08/the-difference-in-five-modes-in-the-aes-encryption-algorithm/ (Accessed: November 25, 2022).

Understanding hashing in cryptography (no date) *Section*. Available at: https://www.section.io/engineering-education/understand-hashing-in-cryptography/#what-is-hashing (Accessed: November 25, 2022).

Ibeakanma, C. (2022) *What is salting in password security and how does it work?*, *MUO*. Available at: https://www.makeuseof.com/what-is-salting/ (Accessed: November 25, 2022).

Ibeakanma, C. (2022) *What is peppering in password security and how does it work?*, *MUO*. Available at: https://www.makeuseof.com/what-is-peppering-how-does-it-work/#:~:text=Peppering%20is%20a%20cryptographic%20process,password%20is%20called%20a%20pepper (Accessed: November 25, 2022).

Mignano, S. (2022) *9 reasons you should be using a password manager*, *Doherty Associates*. Available at: https://www.doherty.co.uk/blog/the-benefits-of-a-password-manager (Accessed: November 25, 2022).

Password manager - logmeonce (no date). Available at: https://www.logmeonce.com/password-manager/ (Accessed: November 25, 2022).

Thakkar, M. (2022) *Sha 256 algorithm explained by a cyber security consultant*, *InfoSec Insights*. Available at: https://sectigostore.com/blog/sha-256-algorithm-explained-by-a-cyber-security-consultant/ (Accessed: November 25, 2022).

KnowBe4 (no date) *What is phishing?*, *Phishing*. Available at: https://www.phishing.org/what-is-phishing (Accessed: November 25, 2022).

Spear phishing (no date) *Definition*. Available at: https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing (Accessed: November 25, 2022).

What is malware? - definition and examples (2022) *Cisco*. Cisco. Available at: https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/what-is-malware.html (Accessed: November 25, 2022).

Kaspersky (2022) *What is malware and how to defend against it?*, *usa.kaspersky.com*. Available at: https://usa.kaspersky.com/resource-center/preemptive-safety/what-is-malware-and-how-to-protect-against-it (Accessed: November 25, 2022).

Thornton, A. (2021) *Business email compromise: What it is, and how to stop it*, *On the Issues*. Microsoft. Available at: https://news.microsoft.com/on-the-issues/2020/07/23/business-email-compromise-cybercrime-phishing/ (Accessed: November 25, 2022).

What is Bec? - business email compromise defined: Proofpoint us (2022) *Proofpoint*. Available at: https://www.proofpoint.com/us/threat-reference/business-email-compromise (Accessed: November 25, 2022).

Ransomware (no date) *Ransomware | Cyber.gov.au*. Available at: https://www.cyber.gov.au/ransomware#:~:text=Ransomware%20is%20a%20common%20and%20dangerous%20type%20of,same%20way%20as%20other%20malware%20or%20a%20virus. (Accessed: November 25, 2022).

What is ransomware? (no date) *IBM*. Available at: https://www.ibm.com/topics/ransomware (Accessed: November 25, 2022).

What is Social Engineering: Attack Techniques & Prevention Methods: Imperva (2019) *Learning Center*. Available at: https://www.imperva.com/learn/application-security/social-engineering-attack/ (Accessed: November 25, 2022).

What is Social Engineering in cyber security? (2022) *Cisco*. Cisco. Available at: https://www.cisco.com/c/en/us/products/security/what-is-social-engineering.html#~related-topics (Accessed: November 25, 2022).