HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 4 (2023)

Cryptography to Prevent Counterfeiting

Arnav Ashok[1] and Richard Stern[#]

[1]Santa Clara High, USA
[#]Advisor

ABSTRACT

In this paper, we introduce a novel approach to identify counterfeit products. We discuss using public/private cryptography to identify the most prominent counterfeit items: drugs, paintings, currency, and luxury items. These items have massive implications on the economy, and in the case of counterfeit drugs, can even lead to death. Identification of these items would lead to the impracticality of counterfeiting and having its negative effects mitigated or prevented.

Introduction

Counterfeiting as an industry is responsible for the loss of billions of dollars for businesses. The four main items that are forged or counterfeited on a daily basis are drugs, paintings, luxury bags and currency. Counterfeit paintings, currency and luxury bags can result in businesses losing thousands of dollars, while counterfeit drugs can result in life threatening health effects. In addition, currency counterfeiting can lead to major negative implications on the economy such as high inflation rates devaluing the currency. It is estimated that around one in five luxury items advertised on instagram are counterfeit (World Economic Forum)[1] and around half of all paintings are forged (Fine Arts Expert Institute)[2]. In developing countries, 1 in 10 drugs are counterfeit and it's estimated to be between a 200 and 440 billion dollar a year industry(NCBI)[3]. Counterfeit items also cause substantial losses for both the artists and businesses. This demonstrates the necessity to find a relatively simple way to distinguish between counterfeit and original items. In this paper, we provide a novel approach that uses cryptography to deter counterfeiting.

Background on Cryptography

Cryptography is the most common method of keeping data secure and the basis of cybersecurity. The essence of cryptography is the ability to send a message that cannot be read by anyone else except for the recipient and the sender. This is done through a process called encryption and decryption. Encryption is the process of changing a message that can be understood by anyone into a code by applying an algorithm to it. Decryption is reverting this code back to the original message through the same algorithm.

One of the common ways of doing this is through a key, which is a set of binary digits that only the sender and recipient have access to. The key and the message are both entered into the algorithm to produce the new encrypted message. This means that messages with a different key will lead to different encrypted versions of those messages. After the message is encrypted, the recipient can decrypt it using the same algorithm and same key.

For example, if a sender wanted to send a secure message to a recipient without anyone else understanding the message, they would send the encrypted version of the message using a particular key and the recipient would use the same key to decode that message (Figure 1).

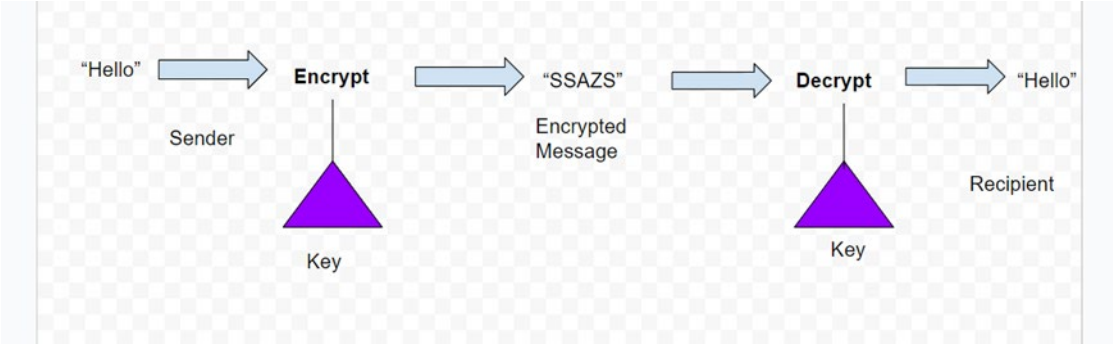

Figure 1. Symmetric Key Encryption

This can work in a system where there are only two people present. This can be a problem when one party is sending a secure message to multiple recipients. If many people have access to the same key, there is a major security risk since those people can modify (forge) the message and it would not be authentic. To solve this issue, one can use a public/private key messaging system (NIST)[5] (Figure 2).

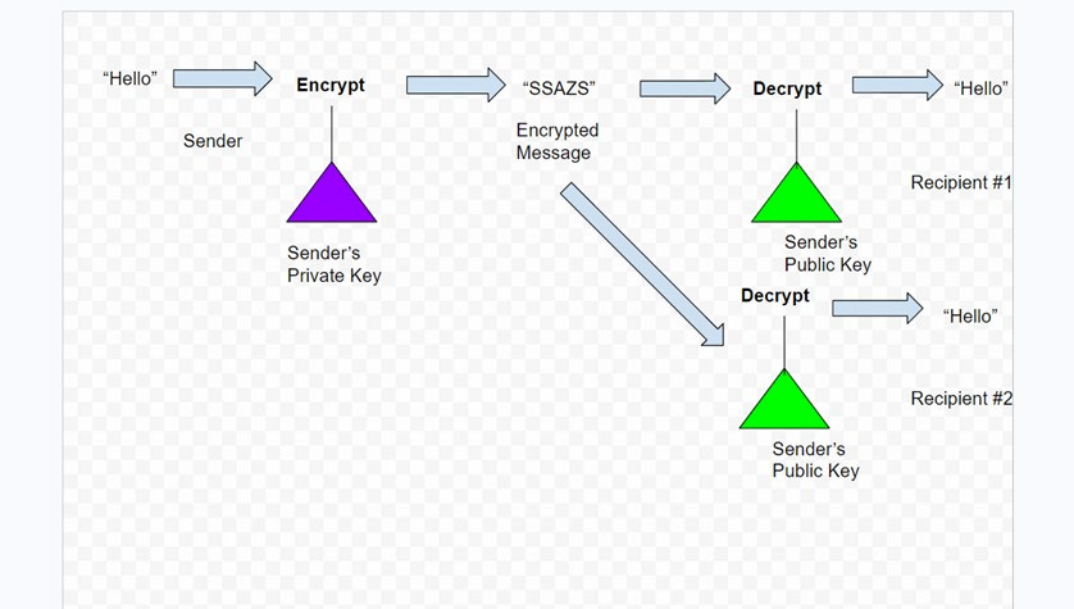

Figure 2. Public/Private Key Encryption

In this system, the sender has a public and private key. The public key is known to all and can be accessed by everyone, while the private key is only known by the sender. The sender would use their private key to encrypt the message. The recipients would use the public key of the sender to decrypt this message. The public key can only be used to decrypt the message, and cannot be used to encrypt. Thus, the recipients would be able to decrypt the message but would be unable to encrypt or forge a message since they do not have access to the private key of the sender. The most widely used algorithm for this purpose is RSA (Rivest-Shamir-Adleman)[4]. Although cryptography and encryption is most commonly used to secure data, it can also be used to prevent counterfeiting through its secretive attributes.

Distinguishing Between Counterfeit Drugs

In order to prevent counterfeiting of drugs, a code can be put on the pill that consists of the date, pill serial number, manufacturer, and the drug name. This serial number will be 128 bits, meaning it will consist of 128 digits, with each being either 0 or 1. The encrypted version of the serial number will also be at the bottom of the pill, which will be encrypted through the company using its private key as shown in figure 3.

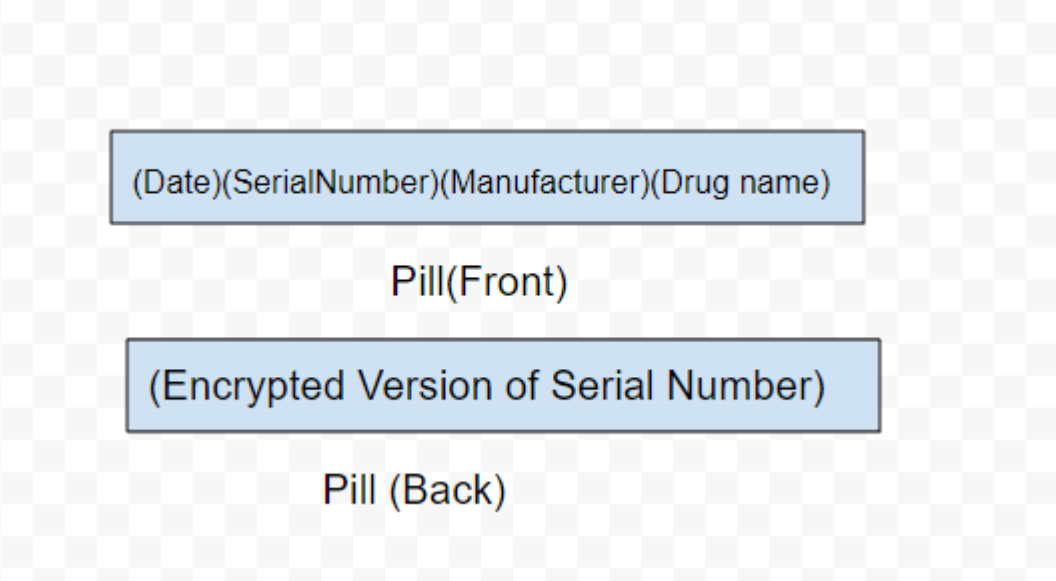

Figure 3. Pill back and Front

In order to verify that the pill is real, the consumer will use the public key of the company to decrypt the encrypted version of the serial number. If this result matches the serial number on the top of the pill, the consumer knows that the pill's serial number comes from the manufacturer. After this, the consumer will enter the encrypted version of the serial number on the back of the pill into the manufacturer's website which will "redeem" the pill (This can happen automatically through the company's app). (Figure 4). This means that the serial number of that pill will be deleted from the company's database and if someone else tries to redeem the same code, a message saying that it has already been redeemed will pop up. As a result, if potential counterfeiters try to stamp the same serial number and encrypted version of the serial number onto fake pills, they can only sell one fake pill for every one real pill they have as once the serial number on the fake pill is redeemed, other pills with the same serial number will be deemed invalid. However, if a counterfeiter decides to use the same serial number on multiple pills, people will begin redeeming invalid codes. This means it is extremely easy to find the counterfeiters who attempt to forge these drugs, as an invalid drug code means it has been counterfeit. An additional layer of security here could also be to make sure the consumer redeems and consumes a pill inside the area they bought the pill, so they are able to identify whether it is counterfeit or not right there (figure 4).

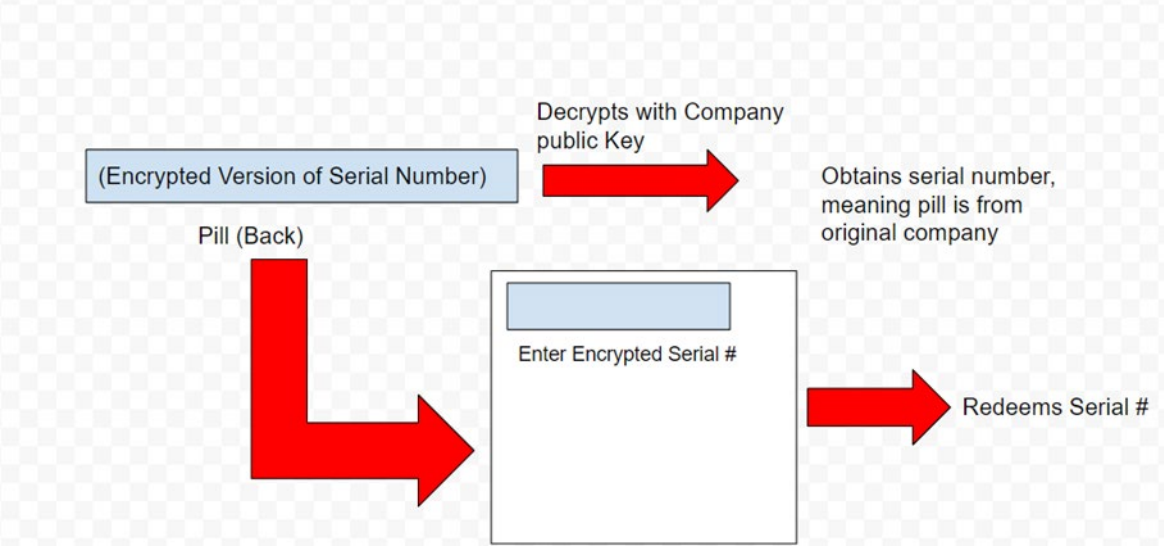

Figure 4. Process of redeeming pill

As a result, counterfeiting drugs would not be a profitable endeavor for these counterfeiters. It is also impossible for a counterfeiter to put random serial numbers on pills as there are 128 bits in the serial number and the chance of a counterfeiter guessing a serial number that exists is lower than the chance of winning 4 lottery ticket jackpots in a row (around 1 in 10^38).

Alternatively all of this data can be stored using qr codes. When a consumer wants to use the pill, they can scan the qr code on the company's website to verify that it is a real pill. Once scanned and verified as a real pill, the same qr code will not be usable again as it has been consumed. This ensures that it is not possible for people to take fake pills and put the same qr code on those pills and sell them to other people. Although customers still have the risk of losing money in buying fake pills, the health risks involved are mitigated. This also allows the real manufacturer and distributor of the pills to profit as more customers will buy the real pills rather than fake ones. Although there are currently qr codes on the bottle of the pills, it is still possible for others to put fake pills into bottles which is why putting it on the pill itself is necessary.

Distinguishing Between Original and Counterfeit Art

For original paintings, the artist usually has their name, title, date, on the back of the painting. The artist can encrypt these elements concatenated together. This means that the name, title, and date of the painting can be concatenated together and then encrypted as a whole using the artist's private key which only they have access to. The encrypted result will be the serial number of the painting. The consumer decrypts the serial number using the artist's public key (Figure 5). Once a consumer buys the painting from the original artist they need to verify that the public private key system is working through decrypting the serial number using the public key. If the painting is resold, the new buyer would have to use the same public private key system to verify it comes from the original artist. Namely, the new buyer would have to decrypt the serial number using the artist's public key and verify it matches the name, date, and title of the painting concatenated together. If the decrypted version of the serial number does not match, they know they do not have the original painting, and the transaction would not go through.

Although this method does make it significantly harder to forge a painting, it is still possible if the forger has the serial number of the painting. However, as long as the serial number is only disclosed to a new buyer, and these transactions are kept track of it is highly impractical to forge paintings as one would have to

own that same painting at one point to forge it. Although this system itself is secure, one extra security measure would be to keep the ownership of paintings public to be stored on a website, where an artist's name can be searched up to see who are the owners of their works. As a result, it becomes highly impractical to forge or replicate art even with knowledge of the serial number of a painting as people who are buying the painting will verify who owns the painting at that time. And if the person who owns the painting at a certain time decides to sell a forged replica of it with the respective serial number of that painting on the back, the painting will be registered to a new owner, and their original painting is unable to be sold. This makes forgery a zero sum game for these forgers and diminishes the value of painting forgery completely.

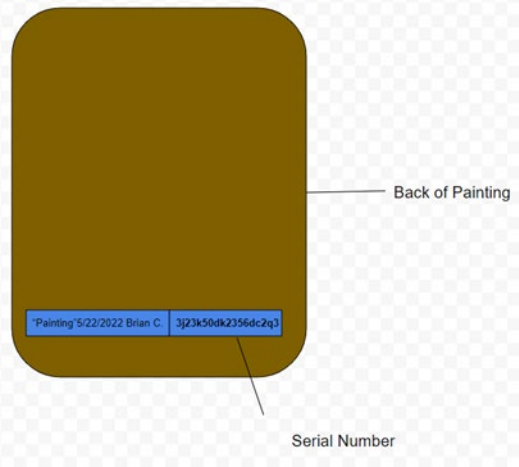

Figure 5. Back of Painting

Distinguishing Between Fake and Original Bags

For luxury bags, the company can have a serial number and the encrypted version of the serial number on the bottom of the bag. This serial number would be encrypted through the company's private key that no one has access to except the company. The company will also have a public key, which allows anyone to decrypt the encrypted text created from the company's private key. Customers can then use the public key to decrypt the encrypted version of the serial number and verify it matches the actual serial number. In order to ensure privacy of these codes, they can have something that only the cash registers can remove that covers the encrypted version of the serial number.

Companies that sell luxury items can also have websites to transfer ownership of items and verify the items' authenticity. Buyers who own items from the company create an account on the website. This account can keep track of ownership of items and allow for items to be transferred to other people. Once a customer buys an item from the store of the company, they can enter in the serial number and its encrypted version on the bottom of the bag and the exact item which is noted by its serial number will be stored in the account "storage". This same serial number can not be redeemed again as it is already stored in someone's account. As a result, it is not possible for one to buy a luxury bag and just use the same serial number along with encrypted version of the serial number and imprint these onto a fake bag to sell. Ownership of items in these accounts can allow for ease of reselling. The transfer process can work through one account sending an item to another account under a sale. This ensures that the buyer knows the item being sold is not counterfeit. For example, if a user with the account number of "1" wants to send someone with the account number of "2", all that is necessary is for the person to enter in the account number "2" as who they want to transfer ownership to and then select the item they want to transfer. As this account number is unique, the user with account number 2 is

the only person who will be able to receive this bag. Although one can buy an actual luxury bag and create a counterfeit bag with the same serial number and encrypted version of it, it is very impractical as they would have to keep buying luxury bags to supply their sales. This system would also not result in profits in dollars as the original bags they own cannot be sold as the ownership does not belong to them in the website anymore. Furthermore, it would not be possible to copy the code on the bag in the store as the bag has to be bought from a store to have ownership on the website. A price at which these luxury items can be considered worth implementing this system in would be over 250 dollars, as otherwise it may be financially inviable. This would serve as a highly effective security measure in preventing counterfeiting.

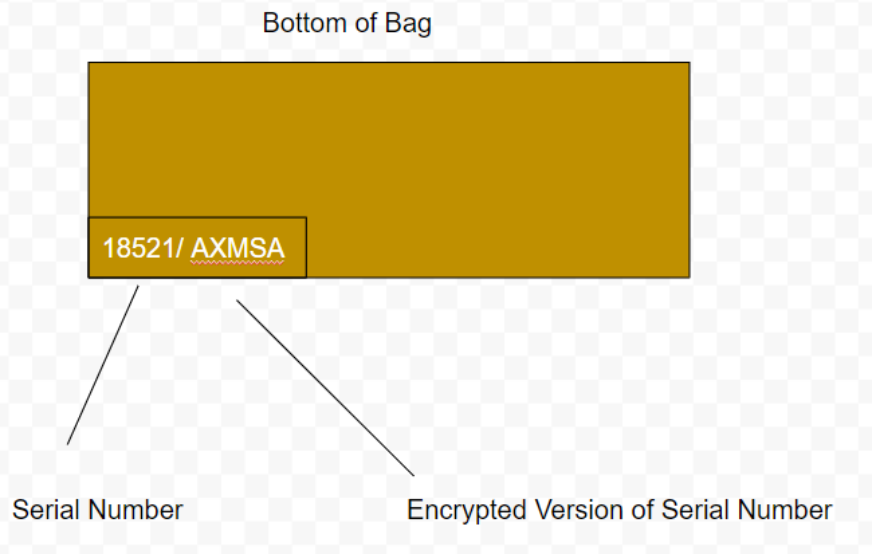

Figure 6. Bottom of Bag

Currency

Mass counterfeiting of currency can have massive negative implications on a government's economy. As a result, it is necessary to have high security measures to prevent counterfeiting from becoming prominent in society given its implications to the economy. A solution is to have an encrypted version of the serial number on the bill using a private key from the government. The public key for the government can be used to decrypt this encrypted version of the serial number. As a result, if one uses the public key of the government to decrypt this encrypted version of the serial number, it should match the actual serial number on the bill, ensuring that the serial number comes from the government and is legitimate.

This process of decrypting the encrypted version of the serial number would be automatic, and occur after any transaction, potentially through a scanner to verify the authenticity of bills. In addition, the serial number of these bills can start with certain numbers or letters to indicate the currency value that is imprinted on the bill. For example, a one dollar bill can have all serial numbers start with AA, or a 5 dollar bill can have all serial numbers start with BB. As a result, counterfeiters who attempt to imprint serial numbers of real dollar bills and their encrypted versions onto fake bills will need to have a bill of the same real value. This makes it much harder to mass produce 100 dollar and 20 dollar bills. Even if one attempts to counterfeit in such regard, the process is highly impractical as using too much of the same serial number will be noticed by these scanners. Scanners can have features where they can track up to the last 100 dollar bills entered into the system and determine if any of them have the same serial number. If these scanners notice a repeat serial number, it can be determined to have a high chance of being counterfeit. As a result, the counterfeiter has to keep using different

legitimate serial numbers on fake bills for this to work, which means it is not possible to counterfeit in masses. As a result, although this method does not completely prevent counterfeiting, it ensures counterfeiting is not able to have a massive effect on the economy due to counterfeiters inability to produce bills in mass quantities.

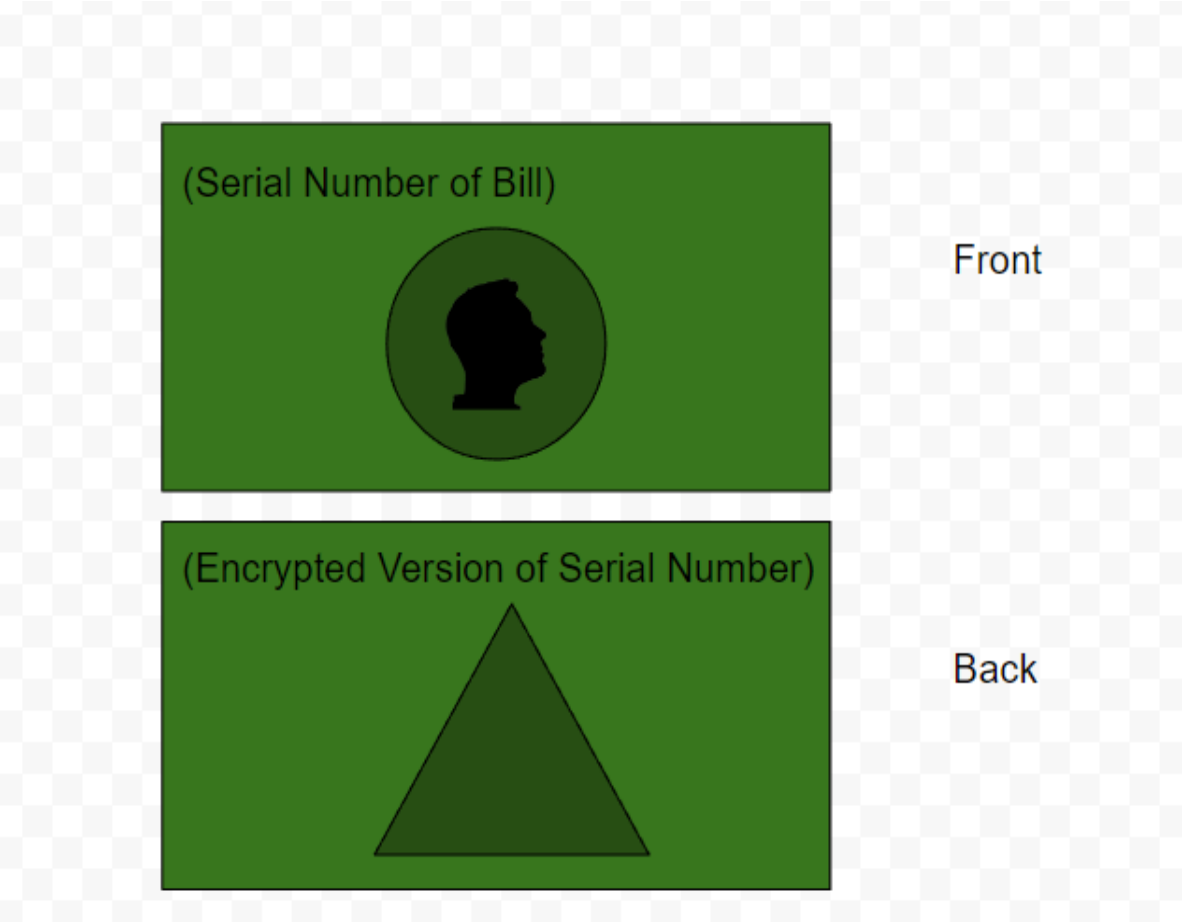

Figure 7. Front and Back of Currency with serial Number

Conclusion

Distinguishing between counterfeit and legitimate items is both scalable and easy to implement. This idea works on luxury items, drugs, currency, and paintings. Additionally, producers of these products (companies or artists) can have a website which can determine ownership of items through redeeming the encrypted message on these items, similar to a gift card. This solution makes counterfeiting of these items on a large scale extremely difficult and highly impractical, resulting in minimal losses to both the consumer and producer.

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

1. Stroppa, A. (2016, June 2). *Instagram is filling up with fake goods. and organized crime's the winner*. World Economic Forum. https://www.weforum.org/agenda/2016/06/instagram-is-filling-up-with-fake-goods-and-organized-crime-s-the-winner/

2. Bambic, A. (2014, October 9). *Art forgery - more than half of art is fake?*. Widewalls. https://www.widewalls.ch/magazine/more-then-half-of-art-is-fake

3. Pathak, R., Gaur, V., Sankrityayan, H., & Gogtay, J. (2023, July). *Tackling counterfeit drugs: The challenges and possibilities*. Pharmaceutical medicine. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10184969/#:~:text=In%202017%2C%20the%20WHO%20estimated,as%20%24200%20billion%20%5B6%5D.

4. Zeki, A., Muhammad, S. J., & Tijjani, B. I. (2014, June). *Cryptanalytic attacks on rivest, Shamir, and Adleman (RSA) cryptosystem ...* ResearchGate. https://www.researchgate.net/publication/277324712_Cryptanalytic_Attacks_on_Rivest_Shamir_and_Adleman_RSA_Cryptosystem_Issues_and_Challenges

5. Editor, C. C. (n.d.). *Home: CSRC*. CSRC Content Editor. https://csrc.nist.gov/