The Evolution of Encryption: DES, AES, and RSA

Levi R. Seibert

Athens State University

ITE 523: Cryptography and Network Security

Dr. Yahia Fadllala

March 15, 2023

The Evolution of Encryption: DES, AES, and RSA

Cryptography is a concept that has been growing in awareness among the general public. This likely a result of the fact that privacy and security are increasingly becoming important factors to the everyday person. In today's technological world, hackers loom behind every corner, hiding in the unknown to harvest just a portion of the data travelling across the information highway. To protect against these malicious actors, data that is sent across the Internet is often encrypted using some version of cryptographical algorithm. There are many algorithms that are used to produce secure transportation of data.

Cryptographical algorithms can be broken down into two major fields: symmetric and asymmetric cryptography. Their differences will be explained shortly. In this report, two symmetric algorithms, namely the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are considered, as is RSA, an asymmetric algorithm. Besides comparing the general details of these three ciphers, this report will analyze some more detailed factors and hypothesize the results of changing certain aspects of the algorithms. Professor Christof Paar's "Introduction to Cryptography" lecture series (available on YouTube) was used as a primary reference tool in the research for this study. This is a highly recommend resource for anyone who is interested in understanding cryptography at an in-depth level, yet explained in a way that is easy to understand.

Introduction to Cryptographical Algorithms

Symmetric vs. Asymmetric

Cryptographical algorithms, or ciphers as they are commonly known, are typically broken down into two overarching subgenres: symmetric and asymmetric. A symmetric cipher is one where a single key is used for the sender and receiver. This key works to both encrypt and decrypt the message (this concept is based on the fact that the logical exclusive-or (XOR) function is reversable). Since only one key is involved in the algorithm, the largest problem with symmetric algorithms is the necessity of sharing

this key with both actors, without any malicious individuals having access to it. Therefore, some type of secure key-sharing mechanism has to be in place.

Asymmetric cryptography avoids this issue by using two different keys. Each entity involved in the cryptological process has a public key (made freely available and well-known) and a private key, which must not be shared with anyone. This is a bit more complex that symmetric cryptography, but the complexity is often worth it; asymmetric cryptography is a very popular choice among ciphers and has been implemented in various applications, such as web certificate checking.

It is also important to point out that DES and AES are both examples of block ciphers, meaning that they encrypt "blocks" or sections of plaintext at a time. This is in contrast to stream ciphers which encrypt data bit by bit. These two smaller genres of ciphers are versions of symmetric algorithms, not asymmetric. RSA is not really either a stream cipher or a block cipher. As will be observed shortly, encryption for RSA is performed using mathematical operations on the plaintext as a whole.

DES

The Data Encryption Standard, or DES, is a symmetric cipher. It was developed by a research team from IBM in the late 1970s. DES is not overly complex, as it makes use of a feistel network (feistel networks are a standard pattern of cryptography) consisting of 16 identical rounds. This design makes taking the inverse of the encryption to be simplistic (if the key is known), thus making decryption an easy task for those with the right permissions. DES is a block cipher and it encrypts 64-bit sections of plaintext into 64-bit sections of ciphertext.

Unfortunately, DES is not very secure. For around twenty years, it was considered the gold standard of encryption (in fact, it was the first standardized encryption algorithm). However, it was discovered that the 56-bit key length of DES is vulnerable to brute force attacks. Even though these attacks take several hours to break a cipher, any cipher that can be broken is not secure. (Introduction to Cryptography by Christof Paar, 2014a).

AES

The search for a replacement of DES began in the 1990's as researchers realized that DES was not going to remain secure. Sophisticated equipment began to brute force the key (over very long periods of computation) and thus proved DES' vulnerableness. In response, NIST put out a call for a 5-year search to find the perfect replacement of AES. The Rijndael cipher was ultimately selected and with some slight modifications, became today's Advanced Encryption Standard, which is still considered secure and is the current gold standard of modern encryption. AES, like DES, is a block symmetric cipher and it encrypts 128-bit blocks of plaintext at a time. AES is very secure, and, to date, there are no known attacks that can exploit AES, thus making it one of the most popular standards of encryption in today's world (Introduction to Cryptography by Christof Paar, 2014c).

RSA

Unlike DES and AES, RSA is an asymmetric algorithm, meaning that there are two keys for each entity. RSA is actually very simple when it comes to encryption and decryption; however, some of the values that must be obtained to encrypt and decrypt the ciphertext are difficult to produce and physically impossible to brute force. RSA stands for Rivest-Shamir-Adleman, a combination of the names of the three authors of the algorithm (Introduction to Cryptography by Christof Paar, 2014d).

Detailed Exploration of Algorithms

DES

As was previously mentioned, DES is a feistel network cipher. However, before and after the 16 feistel rounds, there is a permutation that occurs (referred to as IP for the precursor permutation and IP^{-1} for the successor permutation). The complete DES algorithm is fully reversible, and IP^{-1} is just the inverse of IP. The permutations basically "undo" each other (Introduction to Cryptography by Christof Paar, 2014a).

In addition, before the feistel network can be fully discussed, the key schedule of DES must be considered. DES technically accepts a 64-bit key; however, every eighth bit is used for parity checking and is in effect dropped from the key schedule, therefore making DES' effective key length to be 56 bits (this how DES is commonly characterized). After the 8 bits are dropped, the key is split into two 28-bit sections referred to as *C* and *D*. For each round of the feistel network, each of the two halves are rotated by either one or two bits (one bit for rounds 1, 2, 9, and 16 and two bits for all the others). Finally, for each round, the 56 bits of the key are permuted to produce 48 bits of a key variation and the other 8 bits are dropped (Introduction to Cryptography by Christof Paar, 2014b).

For the actual DES encryption feistel network, the 64-bit block is broken into two sub-blocks, referred to as *L* and *R* (for left and right). For each of the 16 rounds, the value of *L* is XORed with the result of a function, called the *f* function (described below). The result of this XOR operation becomes the next round's *R*, while the current *R* becomes the next round's *L*. This means that during a single round of encryption, half of the plaintext block, namely *R*, is not encrypted in any way (although it does serve as input into the other half's encryption); however, because the halves are swapped, the block section will eventually get encrypted.

The *f* function consists of four operations. First, the 32 bits from *R* are enlarged using an expansion/permutation table to create 48 bits in a new arrangement. Then, these 48 bits are XORed with the corresponding 48-bit subkey for the round, described above. Third, the resulting block is split up into 8 sub-blocks of 6 bit each and each sub-block is fed into a separate substitution box. These tables turn the 6-bit inputs into 4-bit outputs (based on a predefined table). Finally, the 8 sub-blocks of 4 bits each are connected back together and fed into another permutation table to rearrange the order. This 32-bit sequence is what is used to perform the XOR operation with *L* (Introduction to Cryptography by Christof Paar, 2014a).

Decryption of DES consists of just performing the same steps as encryption, in reverse order. The XOR with the *f* function is the root of the encryption, and XORs are reversible, so the plaintext is easily recovered (Introduction to Cryptography by Christof Paar, 2014b).

It is important to note that all of the permutations and substitution boxes for DES are publicly available. While they are not necessarily complex, the tables seem to be chosen at random and don't appear to have much intentionality. Regardless of the reasoning behind the tables being selected the way that they are, DES' encryption was significant and, for the time that it was implemented, was revolutionary. DES is no longer secure, but its insecurity is what has led the technological world to search for what is better. In a very real and literal sense, AES is secure because DES is not.

AES

AES is similar to DES in that is a symmetric cipher, however it does not use a feistel network and has a slightly more complex algorithm. It still does consist of rounds, but the number of rounds is dependent on the key length that is chosen for the encryption (the key can be either 128, 192, or 256 bits). If the key is 128 bits long, then 10 rounds are used, if it is 192 bits, then 12 rounds, and if the key is 256 bits long, then 14 rounds are used.

The very first (and last) step of the AES algorithm is the adding of a subkey. The subkeys used for the initial and final steps, as well as for each of the rounds of the cipher are determined by a complex, multi-step key schedule. Also, before the rounds begin, the 128-bit block is split into 16 groups of 1 byte (8 bits) each.

For each of the rounds of AES (either 10, 12, or 14), a series of 4 steps is performed. First a Byte Substitution is performed, where each byte of the text is run through substitution boxes in parallel, meaning that based on the input bytes, predetermined bytes are outputted, all at the same time. Next, the bytes are reordered with a permutation (this is referred to as the Shift Row step). Thirdly, the Mix Column step reorders the bits within 4-byte blocks of the text, using matrix multiplication. Finally, the

Key Addition step XORs the 128 bits from the AES round with that round's 128-bit subkey from the key schedule. The specifics of each of these steps, or "layers" is quite detailed and requires some more complex mathematics including Galois Fields, but it is sufficient to know that they are orderly and were designed with intentionality, in such a way that they are still secure today (Introduction to Cryptography by Christof Paar, 2014b).

Decryption occurs by implementing each round in reverse order on the ciphertext, with some slight modifications to compute the inverse of some of the steps (GeeksforGeeks, 2022).

RSA

As previously mentioned, RSA is actually quite simple when it comes to encryption and decryption. RSA is a very mathematical-heavy algorithm that relies solely on algebraic computations, but once the mathematics are computed, the algorithm is elementary. Two values, typically referred to as *e* (for encryption) and *d* (for decryption) are calculated. In order to encrypt a plaintext, the plaintext is raised to the power of *e*, and to decrypt a ciphertext, the ciphertext is raised to the power of *d*. Obviously, *e* and *d* have to be related. In fact, *d* is actually the inverse of *e*.

To calculate *e*, an entity needs to choose two very large prime numbers (each needs to be greater than 2^{512}). These two primes are often referred to as *p* and *q*. Next, a value, known Φ(x) is calculated as being equal to $(p - 1) * (q - 1)$. Once this value is known, the public key can be computed. The public key, *e*, is some integer value that is chosen to fulfill two important criteria: *e* must be less than Φ(x), and its greatest common divisor with Φ(x) must be 1 (this means that *e* and Φ(x) must be coprime). The private key, *d*, is just the inverse of the public key, calculated using the Extended Euclidean Algorithm (Introduction to Cryptography by Christof Paar, 2014d). See *Extended Euclidean Algorithm* (n.d.) for an explanation of this algorithm.

Cryptographical Assessment

DES

DES' downfall lies in the fact that its key is too short with only 56 bits of usefulness. Because of this, one might think that simply increasing the key length for DES would make it secure. As is the case with any cipher, longer keys are safer; however, 56 bits of length is nowhere near close to what is necessary for security. 128 bits is pretty much the minimum and this is over double the original length, meaning that DES would have to have some other major modifications to allow for a valid key length. Not only would the algorithm have to be modified, this change would exponentially slow down the cipher and cause unnecessary delays.

An alternative to increasing the key length could be to change the block size of DES. Decreasing the block size from 64 bits to some smaller value would be dangerous, as there would be fewer bits to work with and the subkey would be more apparent. For example, there would be less bits for substitution tables and thus less possible outputs. In its current state, the *f* function has substitution "boxes" that accept 8 groups of 6 bits and substitutes them for 8 groups of 4 bits. With 4-bit strings, there are 16 possible orderings of bits; however, if these outputs were reduced to 3-bit strings, then there would only be 8 possibilities (cutting the uniqueness in half). This would make cryptanalysis easier and let an attacker have a better chance at "reverse engineering" the ciphertext.

Contrarily, the block size could be increased to a larger number. Considering the disadvantages of decreasing the blocks, increasing the blocks sounds like a logical option to increase security. It likely would be helpful, but it would not necessarily change the brute force vulnerability with the key. In addition, changes to the algorithm would have to be done in large multiples of two in order to keep the algorithm in place, so the result could be exponential delays in the processing of the encryption and decryption and thus may not be of much use.

AES

AES is fully secure and has yet to be broken. The stronger versions of the algorithm, such as when 256-bit keys are used, are acceptable for use with TOP SECRET communications. Once again,

increasing the key length would further enhance the algorithm's strength; however, much more than 256 bits could become tasking on the operating system. That is not to say that it would be useless, but since there is no way of brute forcing AES, adding to the key length won't necessarily help accomplish anything.

Modifying the block size could influence the security of AES. A smaller block size would mean that more implementations of the algorithm have to be performed, which would cause the key to be used for frequently and perhaps make it more visible, similar to DES. Also like DES, increasing the block length would cause more complex computations and thus slow down the algorithm. This may be worthwhile; however, since there are no known attacks against AES, it probably is unnecessary for the time being.

RSA

RSA is also fully secure, but its security comes from a completely different aspect; rather than having a complex, really long key, it relies on mathematical calculations. The length of the two selected prime numbers does have an influence on the strength of RSA, but since there is no technical maximum value for the primes there isn't really any way of extending the key length. Similarly, since RSA is not a block cipher, you cannot modify the block sizes to strengthen the cipher. One thing that could be done to increase RSA security without dramatically changing its simplistic algorithm is increase the minimum values of p and q.

Conclusion

DES is not secure; it perhaps could be strengthened by increasing its key length but this would require a reworking of the algorithm. AES and RSA are both fully secure and there is no need to try to increase the key length (which isn't really possible with RSA). DES and AES could have modifications of their block sizes; but the result in strengthen the ciphers would likely be meniscal, at best. There is a reason the ciphers were designed the way that they are, and any changes made to them is risky.

Cryptography is an evolving process. Things that were secure yesterday are not secure today. Right now, AES and RSA are secure algorithms that are acceptable for use. This was once thought true for DES. It is likely true that one day, AES and RSA will no longer be secure. This should not be a cause for panic; as today's technological world gets more complex, the algorithms that secure will also have to get more complex. The issues that are found with one algorithm are fixed in the next, and therefore, as encryption evolves, security should become stronger.

References

Extended Euclidean Algorithm. (n.d.). http://wwwmath.ucdenver.edu/~wcherowi/courses/m5410/exeucalg.html

GeeksforGeeks. (2022, February 11). *Advanced Encryption Standard AES*. https://www.geeksforgeeks.org/advanced-encryption-standard-aes/?ref=rp

Introduction to Cryptography by Christof Paar. (2014a, January 30). *Lecture 5: Data Encryption Standard (DES): Encryption by Christof Paar* [Video]. YouTube. https://www.youtube.com/watch?v=kPBJIhpcZgE

Introduction to Cryptography by Christof Paar. (2014b, January 30). *Lecture 6: Data Encryption Standard (DES): Key Schedule and Decryption by Christof Paar* [Video]. YouTube. https://www.youtube.com/watch?v=l-7YW06BFNs

Introduction to Cryptography by Christof Paar. (2014c, January 30). *Lecture 8: Advanced Encryption Standard (AES) by Christof Paar* [Video]. YouTube. https://www.youtube.com/watch?v=NHuibtoL_qk

Introduction to Cryptography by Christof Paar. (2014d, January 30). *Lecture 12: The RSA Cryptosystem and Efficient Exponentiation by Christof Paar* [Video]. YouTube. https://www.youtube.com/watch?v=QSlWzKNbKrU