The Advanced Encryption Standard

The *Advanced Encryption Standard*, or *AES*, was selected to be a standard, strong symmetric cipher when DES had outlived its secure lifetime. In this handout, we look at the AES development and selection process, algorithm parameters and what they mean for security, and design aspects that affect both software and hardware efficiency.

1 Background and the Aging of DES

The Data Encryption Standard, or DES, was published as an official U.S. government standard in 1975. DES is a block cipher with a 64-bit block size and a 56-bit key, and time has shown that the design is strong and resists (to a reasonable degree) cryptanalytic attacks that would provide a practical advantage over a brute force attack. Unfortunately, as computing power progressed it became clear in the early 1990's that DES was rapidly approaching the end of its useful lifetime. To understand the original design of DES and the need to replace it, let's examine some basic DES design parameters in the context of "state of the art" technology from the mid 1970's and the early 1990's.

Key Length: A brute force attack on DES requires, on average, testing 2^{55} keys. In the mid-1970, being able to test even a million keys/second without a special-purpose machine would have been very expensive. The first mainstream computer capable of 1 MIPS (million operations per second) was the Vax 11/780, introduced in 1978 at a cost of $150,000, could test around 2,500 (a little over 2^{11}) keys per second. Using this state-of-the-art computer, a brute force attack would take around $2^{55-11} = 2^{44}$ seconds, which is half a million years. Looking beyond "mainstream" computers, in 1977 you could buy a Cray 1 supercomputer for $8.86 million, capable of 160 MIPS. So while it was possible to spend a lot of money and get a faster computer, speeding up a half-million year attack by a factor of 160 doesn't help a whole lot. The bottom line is that any brute force attack that could have been performed in the 1970's would have required special-purpose hardware — general computers simply could not come close to the computational power needed.

Published papers from the early 1980's suggested that a DES key-cracking chip could be built that would test around half a million (about 2^{19}) keys per second, so a single chip could cover half the DES keyspace in roughly $2^{55-19} = 2^{36}$ seconds, or 2000 years. Since brute force can easily be sped up by doing key tests in parallel, using 50,000 of these chips to create a key-cracking machine would reduce the time required to a couple of weeks. While such a machine could have been built in the late 1970's, it would have been very expensive — certainly too

expensive for regular criminals and hackers, but within the realm of possibility for a well-funded national security agency. However, by the early 1990's technology had improved so much that it was clear that cracking DES keys was within the range of a moderately-funded attacker. The Electronic Frontier Foundation demonstrated this clearly in 1998 by building a special-purpose machine named "Deep Crack" that cost under $250,000 and could find a DES key in less than 3 days. More recent work has brought that cost down to under $10,000.

Block Size: So far in this class, we have only talked about using cryptography to protect confidentiality. However, block ciphers can also be used to create message authentication codes or in other settings in which attacks can be performed using space and time proportional to the square root of the size of the plaintext space. Specifically, for this type of attack on a b-bit block cipher, you need to store a table with $\sqrt{2^b} = 2^{b/2}$ entries of b bits each. For a 64-bit block cipher, this is a table with 2^{32} entries, each 64 bits or 8 bytes long, for a total size of 2^{35} bytes, or around 32 GBytes. In 1975, that was astonishingly huge — the largest hard drive at the time was the IBM 3330-II, which stored 200 MBytes, and cost $37,000.

By 1992, 1 GB hard drives were commercially available for a reasonable price, and it was clear that in the next 10 years the 32 GB required for this attack would be readily available and cheap. Therefore, while most people think only of keylength when they think about the security of a block cipher, it was clear in the early 1990's that any replacement would also need to have a block size larger than 64 bits. It is important to note that in the early 1990's, some applications used a triple-application of DES to increase its keysize to a secure level with over 100 bits, but this technique (known as triple-DES or 3DES) still has a 64-bit block size.

2 Parameters for Modern Security

As described above, while the block size and key length of DES were fairly strong at its introduction in the mid-1970's, by the early 1990's it was clear that its days as a secure cipher were numbered. Next we consider what parameters will give strong security now and for the next few decades (at least).

Key Length: Every bit added to the keylength doubles the time required for a brute force attack, so modest keylength increases can significantly increase security. It's not difficult to come up with a reasonable estimate for a secure keylength: The fastest commercial hardware for AES currently available can perform approximately 300 million encryptions per second, so let's be generous and assume we can make a custom chip that performs a billion (approximately 2^{30}) encryptions per second. We will build a huge key cracking machine with a million (approximately 2^{20}) of these chips, so this machine would be capable of testing approximately 2^{50} keys per second with today's technology. If we assume Moore's Law continues for the next 15 years, computing power will have doubled 10 times during that 15 years, so in 15 years we could build a machine that would test $2^{10} \cdot 2^{50} = 2^{60}$ keys per second. And finally, let's say that a key length is secure if it would take more than a thousand years (or 2^{35} seconds) on average

to break. This means that a keyspace of size 2^{96}, or designing for a keylength of 96 bits, will remain extremely secure for the next 15 years, even making some *very* generous assumptions regarding computing power.

Block Size: For design reasons, block sizes are almost always powers of 2 (so 32 bits, 64 bits, 128 bits, 256 bits, ...). We saw above that 64 bits is not secure against today's technology, so consider 128 bits as a block size. By moving to a 128-bit block size, the space needed for the attack described above would be $16 \cdot 2^{64} = 2^{68}$ bytes, or 256 million terabytes. Today (2017), mass storage costs around $35 per TB, so 256 million terabytes would cost around $9 billion — not to mention the cost of housing this storage, powering it, and the necessary interconnections. Thus, 128-bit blocks are easily sufficient for the next few decades. If there are revolutionary breakthroughs in storage technology in the next few decades, then it might be wise to consider moving to 256 bit blocks, but unless we really don't understand physics and the way the universe works we will never have to move beyond 256 bit blocks to protect from the collision attacks that we are considering.

3 AES – The Selection Process

While it was clear that DES was near the end of its useful life in the early 1990's, there was not a clear and well-accepted direction forward taken by US government agencies and standards bodies for a few years. In 1993 the government tried to address the need for stronger encryption in telecommunications (primarily phones) by introducing a product known as the "Clipper Chip," a hardware device that used a classified cipher named SKIPJACK with an 80-bit key. An 80-bit key provides very strong security (roughly 16 million times stronger than DES), and to address the concerns of law enforcement this chip was built to support "key escrow" — essentially, each chip had a unique key that would unlock a "Law Enforcement Access Field" that would allow them to decrypt the communication. Copies of these unique keys would be kept by the government (with certain protections) so that they could be obtained after getting legal clearance. The Clipper Chip proposal was soundly rejected by technology groups and by the general public, and it was completely discontinued by 1996. In 1998 the SKIPJACK block cipher was declassified so that it could be used freely, but it is only rarely used.

It is important to note that in 1975, when DES was adopted, there was very little cryptographic expertise outside of the military. The initial 1973 request for proposals for a data encryption standard did not receive any acceptable submissions, and a second call had to be made (with a specific invitation to IBM) in order to get even one strong algorithm to consider. However, between 1975 and 1993 there was a huge amount of cryptographic research in the civilian science community, and by 1993 there was a lot of expertise and a lot of strong algorithms to use. So while DES was, in some sense, the "only game in town" in 1975, that was far from the case in 1993. This is a large reason why the Clipper Chip proposal, with keys kept by the government, was doomed to failure. This is even more true today (2017), and

with widespread knowledge of strong encryption techniques, any proposal for an escrowed or back-doored encryption system would not provide any benefit, nor would it be accepted.

Seeing the need for a strong, open, and secure replacement for DES, in 1997 the National Institute of Standards and Technology (NIST) announced a competition to choose a successor for DES, which would be called the "Advanced Encryption Standard," or AES. Based on similar reasoning to what we described above, they set the following parameters for submissions to this competition:

- submissions must be block ciphers;
- submissions must use a block size of 128 bits; and
- submissions must support key sizes of 128, 192, and 256 bits.

In response, NIST received 15 submissions, which were published and evaluated by NIST and through two conferences that focused on security and performance (both hardware and software) of the submissions. After roughly two years of analysis, the top five finalists were selected in 1999 for further review. After another year of intense study, an algorithm named "Rijndael" was selected to be the new standard, and the official standards document was published in 2001. While the original Rijndael algorithm supported 5 different block sizes, with 128-bits being the smallest, the AES standard only uses the 128-bit option. Among other justifications, this greatly simplifies hardware design.

There are several important aspects to the selection process for AES that stand out. First, it was an entirely open and transparent process. While the NSA reviewed all finalists, there were no unexplained or classified modifications made as was done with DES. The vast majority of analysis was performed by civilian researchers and the results were openly published. Second, while the competition was run by a U.S. government agency to select a U.S. national standard, it was a highly international process. The winning algorithm, Rijndael, was invented and submitted by two Belgian cryptographers, Vincent Rijmen and Joan Daemen. Third, this was not a rushed process. Partially because of the openness and inclusiveness of the process, the candidates were evaluated for several years before a final selection was made. All of these aspects of the AES selection process have led to a great deal of confidence in the AES algorithm, without the lingering suspicions that followed from DES's process that included modifications made by a secretive U.S. government organization.

4 Additional AES Properties

Beyond the basic parameters for AES (blocksize of 128 bits, and keysize of 128, 192, or 256 bits), there are a few other aspects of AES that are useful to know about.

Strength of the Algorithm: AES has been in widespread use and under intense research scrutiny for around 20 years, since Rijndael was first proposed in 1997. During that time, no significant attacks have been discovered against the full algorithm. Researchers have made progress

against simplified versions (for example, with a reduced number of cipher rounds) or where "breaking" is defined as distinguishing from a random function (which is interesting, but doesn't directly imply a way to attack any important security goal). Currently, the best algorithms known for an attacker to discover a key used by AES are only a factor of 2–4 better than a brute-force search. Given the failure of cryptanalytic attacks against AES, rough brute-force attack estimates as we did above give a good indication of the strength of AES.

Software Efficiency: When the NBS put out its initial call for proposals for DES in 1973, computers were expensive and rare — personal computers had not been introduced, and the general way people viewed (and designed) cryptography was for hardware implementation in a dedicated device. DES contains several operations in which data is manipulated on a bit-by-bit level, including some fairly arbitrary and unstructured bitwise permutations. Moving individual bits around in a hardware implementation is relatively easy — it's just a matter of connecting wires from the input position to the output position. However, on a general-purpose CPU, where the minimum addressable unit is a byte or a word, manipulating individual bits like this is awkward and inefficient. Because of this, DES has always been somewhat inefficient in software, and when attempts were made to strengthen the security by applying DES three times in 3DES, this just magnified the inefficiency.

By contrast, AES was invented when personal computers were wide-spread, and it was clear that any encryption algorithm needed to be designed so that it was efficient in software. In AES, the minimum unit of data operated on is a byte. The operations performed on bytes by AES are standard mathematical operations, but on some processors they might not be directly supported. However, even in that case, they are much more structured and efficient than the bitwise permutations used by DES. Furthermore, as AES is such an important algorithm, most modern processors include special instructions to speed up the operations that AES uses. In Intel and AMD processors, a set of assembly language instructions called the AES-NI instructions can be used to perform AES encryption at incredibly fast speeds, with encryption throughput that is over 10 gigabits per second on a single core.[1]

Use for Classified Data: DES was officially approved for use within the government for sensitive, but not classified data. The fact that DES was not approved for classified data was seen by some as a sign that there was a weakness in the algorithm, or at the very least that the government did not have high confidence in the security of the algorithm. By contrast, in 2003 the U.S. government announced that AES was approved for protecting classified data: 128-bit (or larger) keys were approved for protecting data classified at the SECRET level, and 192-bit (or larger) keys were approved for protecting TOP SECRET data. The fact that the government has approved the algorithm for protecting its most highly-classified secrets is another reason people have high confidence in the strength and security of AES.

[1] A simple speed test shows an encryption throughput of 1.56 gigabytes, or about 12.5 gigabits, per second on a Intel i7-6700 processor. `https://calomel.org/aesni_ssl_performance.html`