

CS 5602 Introduction to Cryptography

Lecture 23

Block Ciphers

George Markowsky

Computer Science Department

Missouri University of Science & Technology

1

Block Ciphers

- The block sizes taken are usually reasonably large, 64 bits in DES and 128 bits or more in modern block ciphers.
- Often the output of the ciphertext produced by encrypting the first block is used to help encrypt the second block in what is called a mode of operation.
- These modes are used to avoid certain attacks based on deletion or insertion by giving each ciphertext block a context within the overall message.
- Each mode of operation offers different protection against error propagation due to transmission errors in the ciphertext.
- In addition, depending on the mode of operation (and the application) message/session keys may be needed.

4

Chapter Goals

- All material not otherwise attributed is from Smart's Book
- To introduce the notion of block ciphers.
- To understand the workings of the DES algorithm.
- To understand the workings of the Rijndael algorithm.
- To learn about the various standard modes of operation of block ciphers.

FIGURE 1. Operation of a block cipher

```
graph TD
    m[Plaintext block m] --> e[Cipher function e]
    k[Secret key k] --> e
    e --> c[Ciphertext block c]
```

2

Block Ciphers

- For example, many modes require a per message initial value to be input into the encryption and decryption operations.
- Later in this chapter we shall discuss modes of operation of block ciphers in more detail.
- There are many block ciphers in use today, some which you may find used in your web browser are RC5, RC6, DES or 3DES.
- The most famous of these is DES, or the Data Encryption Standard.
- This was first published in the mid-1970s as a US Federal standard and soon become the de-facto international standard for banking applications.

5

Block Ciphers

- The main difference between a block cipher and a stream cipher is that block ciphers are stateless, whilst stream ciphers maintain an internal state which is needed to determine which part of the keystream should be generated next.
- We write:
$$c = e_k(m),$$
$$m = d_k(c)$$

where

- m is the plaintext block,
- k is the secret key,
- e is the encryption function,
- d is the decryption function,
- c is the ciphertext block.

3

DES

- The DES algorithm has stood up remarkably well to the test of time, but in the early 1990s it became clear that a new standard was required. This was because both the block length (64 bits) and the key length (56 bits) of basic DES were too small for future applications.
- It is now possible to recover a 56-bit DES key using either a network of computers or specialized hardware.
- In response to this problem the US National Institute for Standards and Technology (NIST) initiated a competition to find a new block cipher, to be called the Advanced Encryption Standard or AES.

6

DES

- Unlike the process used to design DES, which was kept essentially secret, the design of the AES was performed in public.
- A number of groups from around the world submitted designs for the AES.
- Eventually five algorithms, known as the AES finalists, were chosen to be studied in depth. These were
 - MARS from a group at IBM,
 - RC6 from a group at RSA Security,
 - Twofish from a group based at Counterpane, UC Berkeley and elsewhere,
 - Serpent from a group of three academics based in Israel, Norway and the UK,
 - Rijndael from a couple of Belgian cryptographers.
- Finally in the fall of 2000, NIST announced that the overall AES winner had been chosen to be Rijndael (pronounced rain-dahl).

7

Breaking Block Ciphers

- There are a number of general purpose techniques which can be used to break a block cipher, for example: exhaustive search, using pre-computed tables of intermediate values or divide and conquer.
- Some (badly designed) block ciphers can be susceptible to chosen plaintext attacks, where encrypting a specially chosen plaintext can reveal properties of the underlying secret key.
- In cryptanalysis one needs a combination of mathematical and puzzle-solving skills, plus luck.
- There are a few more advanced techniques which can be employed, some of which apply in general to any cipher (and not just a block cipher).

10

Iterated Block Ciphers

- DES and all the AES finalists are examples of iterated block ciphers.
- The block ciphers obtain their security by repeated use of a simple round function.
- The round function takes an n -bit block and returns an n -bit block, where n is the block size of the overall cipher.
- The number of rounds r can either be a variable or fixed.
- As a general rule increasing the number of rounds will increase the level of security of the block cipher.

8

Differential Cryptanalysis

- In differential cryptanalysis one looks at ciphertext pairs, where the plaintext has a particular difference.
- The exclusive-or of such pairs is called a differential and certain differentials have certain probabilities associated to them, depending on what the key is.
- By analyzing the probabilities of the differentials computed in a chosen plaintext attack one can hope to reveal the underlying structure of the key.

11

Iterated Block Ciphers

- Each use of the round function employs a round key k_i for $1 \leq i \leq r$ derived from the main secret key k , using an algorithm called a key schedule.
- To allow decryption, for every round key the function implementing the round must be invertible, and for decryption the round keys are used in the opposite order that they were used for encryption.
- That the whole round is invertible does not imply that the functions used to implement the round need to be invertible.
- This may seem strange at first reading but will become clearer when we discuss the DES cipher later.
- In DES the functions needed to implement the round function are not invertible, but the whole round is invertible.
- For Rijndael not only is the whole round function invertible but every function used to create the round function is also invertible.

9

Linear Cryptanalysis

- Even though a good block cipher should contain non-linear components the idea behind linear cryptanalysis is to approximate the behavior of the non-linear components with linear functions.
- Again the goal is to use a probabilistic analysis to determine information about the key.
- Surprisingly these two methods are quite successful against some ciphers.
- But they do not appear that successful against DES or Rijndael, two of the most important block ciphers in use today.

12


DES and Rijndael

- Since DES and Rijndael are likely to be the most important block ciphers in use for the next few years we shall study them in some detail.
- This is also important since they both show general design principles in their use of substitutions and permutations.
- Recall that the historical ciphers made use of such operations, so we see that not much has changed.
- Now, however, the substitutions and permutations used are far more intricate.
- On their own they do not produce security, but when used over a number of rounds one can obtain enough security for our applications.

13

Donald Coppersmith

- Don Coppersmith (born c. 1950) is a cryptographer and mathematician.
- He was involved in the design of the Data Encryption Standard block cipher at IBM, particularly the design of the S-boxes, strengthening them against differential cryptanalysis.
- He has also worked on algorithms for computing discrete logarithms, the cryptanalysis of RSA, methods for rapid matrix multiplication (see Coppersmith–Winograd algorithm) and IBM’s MARS cipher.
- Don is also a co-designer of the SEAL and Scream ciphers.
- In 1972, Coppersmith obtained a Bachelor’s degree in mathematics at the Massachusetts Institute of Technology, and a Masters and PhD in mathematics from Harvard University in 1975 and 1977 respectively.
- He was a Putnam Fellow each year from 1968–1971, becoming the first four-time Putnam Fellow in history.
- In 1998, he started Ponder This, an online monthly column on mathematical puzzles and problems.
- In October 2005, the column was taken over by James Shearer.
- In 2002, Coppersmith won the RSA Award for Excellence in Mathematics.



16

Block Ciphers vs Stream Ciphers

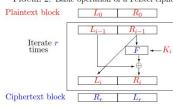
- We end this section by discussing which is best, a block cipher or a stream cipher?
- Alas there is no correct answer to this question.
- Both have their uses and different properties. Here are just a few general points.

1. Block ciphers are more general, and we shall see that one can easily turn a block cipher into a stream cipher.
2. Stream ciphers generally have a more mathematical structure. This either makes them easier to break or easier to study to convince oneself that they are secure.
3. Stream ciphers are generally not suitable for software, since they usually encrypt one bit at a time. However, stream ciphers are highly efficient in hardware.
4. Block ciphers are suitable for both hardware and software, but are not as fast in hardware as stream ciphers.
5. Hardware is always faster than software, but this performance improvement comes at the cost of less flexibility.

14

Feistel Ciphers and DES

FIGURE 2. Basic operation of a Feistel cipher



Plaintext block: L_0, R_0

Iterate r times


Ciphertext block: L_1, R_1

- The DES cipher is a variant of the basic Feistel cipher described in Fig. 2, named after H. Feistel who worked at IBM and performed some of the earliest non-military research on encryption algorithms.
- The interesting property of a Feistel cipher is that the round function is invertible regardless of the choice of the function in the box marked F .

17

Horst Feistel

- Horst Feistel (January 30, 1914?1915 – November 14, 1990) was a German-born cryptographer who worked on the design of ciphers at IBM, initiating research that culminated in the development of the Data Encryption Standard (DES) in the 1970s.
- Feistel was born in Berlin, Germany in 1915, and moved to the United States in 1934.
- During World War II, he was placed under house arrest, but nevertheless gained U.S. citizenship on 31 January 1944.
- The following day he was granted a security clearance and began work for the U.S. Air Force Cambridge Research Center (AFRC) on Identification Friend or Foe (IFF) devices until the 1950s.
- He was subsequently employed at MIT’s Lincoln Laboratory, then the MITRE corporation. Finally, he moved to IBM, where he received an award for his cryptographic work.
- His research at IBM led to the development of the Lucifer and Data Encryption Standard (DES) ciphers. Feistel was one of the earliest non-government researchers to study the design and theory of block ciphers.
- Feistel lent his name to the Feistel network construction, a common method for constructing block ciphers (for example DES).



15

Properties of Feistel Ciphers

- An interesting property of a Feistel cipher is that the round function is invertible regardless of the choice of the function in the box marked F
- To see this notice that each encryption round is given by
 - $L_i = R_{i-1}$
 - $R_i = L_{i-1} \oplus F(K_i, R_{i-1})$.
- Hence, the decryption can be performed via
 - $R_{i-1} = L_i$
 - $L_{i-1} = R_i \oplus F(K_i, L_i) = R_i \oplus F(K_i, R_{i-1}) = R_i \oplus F(K_i, R_{i-1}) \oplus F(K_i, R_{i-1}) = R_i$
- F does not have to be invertible and can be arbitrarily complex

18

Properties of Feistel Ciphers

- This means that in a Feistel cipher we have simplified the design somewhat, since we can choose any function for the function F , and we will still obtain an encryption function which can be inverted using the secret key, the same code/circuitry can be used for the encryption and decryption functions.
- We only need to use the round keys in the reverse order for decryption.
- Of course to obtain a secure cipher we still need to take care with
 - How the round keys are generated
 - How many rounds to take
 - How the function F is defined

19

DES

- DES is also known as the Data Encryption Algorithm DEA in documents produced by the American National Standards Institute, ANSI.
- The International Standards Organisation ISO refers to DES by the name DEA-1.
- It has been a world-wide standard for well over twenty years and stands as the first publicly available algorithm to have an 'official status'.
- It therefore marks an important step on the road from cryptography being a purely military area to being a tool for the masses.

22

Properties of Feistel Ciphers

- This means that in a Feistel cipher we have simplified the design somewhat, since we can choose any function for the function F , and we will still obtain an encryption function which can be inverted using the secret key, the same code/circuitry can be used for the encryption and decryption functions.
- We only need to use the round keys in the reverse order for decryption.
- Of course to obtain a secure cipher we still need to take care with
 - How the round keys are generated
 - How many rounds to take
 - How the function F is defined

20

DES

- The basic properties of the DES cipher are that it is a variant of the Feistel cipher design with
 1. the number of rounds r is 16,
 2. the block length n is 64 bits,
 3. the key length is 56 bits,
 4. the round keys K_1, \dots, K_{16} are each 48 bits.

23

DES

- Work on DES was started in the early 1970s by a team in IBM which included Feistel.
- It was originally based on an earlier cipher of IBM's called Lucifer, but some of the design was known to have been amended by the National Security Agency, NSA.
- For many years this led the conspiracy theorists to believe that the NSA had placed a trapdoor into the design of the function F .
- However, it is now widely accepted that the modifications made by the NSA were done to make the cipher more secure.
- In particular, the changes made by the NSA made the cipher resistant to differential cryptanalysis, a technique that was not discovered in the open research community until the 1980s.

21

3DES

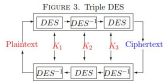
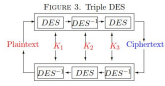


FIGURE 3. Triple DES

- Note that a key length of 56 bits is insufficient for many modern applications, hence often one uses DES by using three keys and three iterations of the main cipher.
- Such a version is called Triple DES or 3DES, see Fig. 3.
- In 3DES the key length is equal to 168.
- There is another way of using
 - DES three times, but using two keys instead of three giving rise to a key length of 112.
 - In this two-key version of 3DES one uses the 3DES basic structure but with the first and third key being equal.
 - However, two-key 3DES is not as secure as one might initially think.

24

3DES



- Wikipedia
- After DES was cracked, the NIST, the US institution for technology and also cryptography, developed 3DES.
- It has 3 times more bits, but is otherwise the same as DES.
- Theoretically, 3DES should provide 168 bits of security.
- But because of the design, the NIST later said it only provides 80 bits of security.
- That can be broken by a modern computer and thus the cipher should be considered broken.

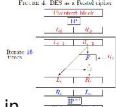
25

The Mysterious Function F

- S-Box: Each six-bit value is passed into one of eight different S-Boxes (Substitution Box) to produce a four-bit result. The S-Boxes represent the non-linear component in the DES algorithm and their design is a major contributor to the algorithms security. Each S-Box is a look-up table of four rows and sixteen columns. The six input bits specify which row and column to use. Bits 1 and 6 generate the row number, whilst bits 2, 3, 4 and 5 specify the column number. The output of each S-Box is the value held in that element in the table.
- P-Box: We now have eight lots of four-bit outputs which are then combined into a 32-bit value and permuted to form the output of the function F.

28

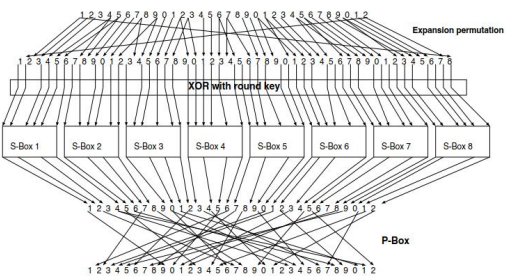
DES Details



- Basically DES is a Feistel cipher with 16 rounds, as depicted in Fig. 4, except that before and after the main Feistel iteration a permutation is performed.
- Notice how the two blocks are swapped around before being passed through the final inverse permutation.
- This permutation appears to produce no change to the security, and people have often wondered why it is there.
- One answer given by one of the original team members was that this permutation was there to make the original implementation easier to fit on the circuit board.

26

FIGURE 5. Structure of the DES function F



29

The Mysterious Function F

- F is calculated in 5 stages (Smart six stages but only gives 5!)
- Expansion Permutation: The right half of 32 bits is expanded and permuted to 48 bits. This helps the diffusion of any relationship of input bits to output bits. The expansion permutation (which is different from the initial permutation) has been chosen so that one bit of input affects two substitutions in the output, via the S-Boxes below. This helps spread dependencies and creates an avalanche effect (a small difference between two plaintexts will produce a very large difference in the corresponding ciphertexts).
- Round Key Addition: The 48-bit output from the expansion permutation is XORed with the round key, which is also 48 bits in length. Note, this is the only place where the round key is used in the algorithm.
- Splitting: The resulting 48-bit value is split into eight lots of six-bit values.

27

IP and IP⁻¹

58 50 42 34 26 18 10 2	40 8 48 16 56 24 64 32
60 52 44 36 28 20 12 4	39 7 47 15 55 23 63 31
62 54 46 38 30 22 14 6	38 6 46 14 54 22 62 30
64 56 48 40 32 24 16 8	37 5 45 13 53 21 61 29
57 49 41 33 25 17 9 1	36 4 44 12 52 20 60 28
59 51 43 35 27 19 11 3	35 3 43 11 51 19 59 27
61 53 45 37 29 21 13 5	34 2 42 10 50 18 58 26
63 55 47 39 31 23 15 7	33 1 41 9 49 17 57 25

30

"Expansion Permutation"

• 32 1 2 3 4 5

• 4 5 6 7 8 9

• 8 9 10 11 12 13

• 12 13 14 15 16 17

• 16 17 18 19 20 21

• 20 21 22 23 24 25

• 24 25 26 27 28 29

• 28 29 30 31 32 1

• Note this is not a permutation exactly because it maps 32 bits into 48 bits

• Notice that the bits which have arrows are used twice

• There are 16 bits that are used twice (red) and 16 bits that are used once (black)

• This gives a total of 48 bits

• First and last bits on each row give the row of the S-box and the other bits give the column

31

S5

S ₅	Middle 4 bits of input																
	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111	
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1101	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

34

<div>S-Box 1</div> <div>14 4 13 1 2 15 11 8 3 10 6 12 5 9 0 7</div> <div>0 15 7 4 14 2 13 11 10 6 12 11 9 5 3 8</div> <div>4 1 14 8 13 6 2 11 15 12 9 7 3 10 5 0</div> <div>15 12 8 2 4 9 1 7 5 11 3 14 10 0 6 13</div>	<div>S-Box 5</div> <div>2 12 4 1 7 10 11 6 8 5 3 15 13 0 14 9</div> <div>14 11 2 12 4 7 13 1 5 0 15 10 3 9 8 6</div> <div>4 2 1 11 10 13 7 8 15 9 12 5 6 3 0 14</div> <div>11 8 12 7 1 14 2 13 6 15 0 9 10 4 5 3</div>
<div>S-Box 2</div> <div>15 1 8 14 6 11 3 4 9 7 2 13 12 0 5 10</div> <div>3 13 4 7 15 2 8 14 12 0 1 10 6 9 11 5</div> <div>0 14 7 11 10 4 13 1 5 8 12 6 9 3 2 15</div> <div>13 8 10 1 3 15 4 2 11 6 7 12 0 5 14 9</div>	<div>S-Box 6</div> <div>12 1 10 15 9 2 6 8 0 13 3 4 14 7 5 11</div> <div>10 15 4 2 7 12 9 5 6 1 13 14 0 11 3 8</div> <div>9 14 15 5 2 8 12 3 7 0 4 10 1 13 11 6</div> <div>4 3 2 12 9 5 15 10 11 14 1 7 6 0 8 13</div>
<div>S-Box 3</div> <div>10 0 9 14 6 3 15 5 1 13 12 7 11 4 2 8</div> <div>13 7 0 9 3 4 6 10 2 8 5 14 12 11 15 1</div> <div>13 6 4 9 8 15 3 0 11 1 2 12 5 10 14 7</div> <div>1 10 13 0 6 9 8 7 4 15 14 3 11 5 2 12</div>	<div>S-Box 7</div> <div>4 11 2 14 15 0 8 13 3 12 9 7 5 10 6 1</div> <div>13 0 11 7 4 9 1 10 14 3 5 12 2 15 8 6</div> <div>1 4 11 13 12 3 7 14 10 15 6 8 0 5 9 2</div> <div>6 11 13 8 1 4 10 7 9 5 0 15 14 2 3 12</div>
<div>S-Box 4</div> <div>7 13 14 3 0 6 9 10 1 2 8 5 11 12 4 15</div> <div>13 8 11 5 6 15 0 3 4 7 2 12 1 10 14 9</div> <div>10 6 9 0 12 11 7 13 15 1 3 14 5 2 8 4</div> <div>3 15 0 6 10 11 13 8 9 4 5 11 12 7 2 14</div>	<div>S-Box 8</div> <div>13 2 8 4 6 15 11 1 10 9 3 14 5 0 12 7</div> <div>1 15 13 8 10 3 7 4 12 5 6 11 0 14 9 2</div> <div>7 11 4 1 9 12 14 2 0 6 10 13 15 3 5 8</div> <div>2 1 14 7 4 10 8 13 15 12 9 0 3 5 6 11</div>

32

The P-Box

• 16 7 20 21

• 29 12 28 17

• 1 15 23 26

• 5 18 31 10

• 2 8 24 14

• 32 27 3 9

• 19 13 30 6

• 22 11 4 25

• Does not seem to match Figure 5

• Permutation of the 8 × 4 = 32 bit outputs produced by the S-boxes

35

S-Boxes (Wikipedia)

• In cryptography, an S-box (substitution-box) is a basic component of symmetric key algorithms which performs substitution.

• In block ciphers, they are typically used to obscure the relationship between the key and the ciphertext — Shannon's property of confusion.

• In general, an S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m.

• An m×n S-box can be implemented as a lookup table with 2^m words of n bits each.

• Fixed tables are normally used, as in the Data Encryption Standard (DES), but in some ciphers the tables are generated dynamically from the key (e.g. the Blowfish and the Twofish encryption algorithms).

• One good example of a fixed table is the S-box from DES (S₅), mapping 6-bit input into a 4-bit output:

33

DES Key Schedule

• We have been talking about a 56-bit key, so where do all the 48-bit keys comes from?

• They are generated from the 56-bit key!

• The DES key schedule takes the 56-bit key, which is actually input as a bitstring of 64 bits comprising of the key and eight parity bits, for error detection.

• These parity bits are in bit positions 8, 16, . . . , 64 and ensure that each byte of the key contains an odd number of bits.

36

DES Key Schedule (PC-1)

- We first permute the bits of the key according to the following permutation (which takes a
- 64-bit input and produces a 56-bit output, hence discarding the parity bits).
- This is called PC-1 in the literature

• 57 49 41 33 25 17 9
• 1 58 50 42 34 26 18
• 10 2 59 51 43 35 27
• 19 11 3 60 52 44 36
• 63 55 47 39 31 23 15
• 7 62 54 46 38 30 22
• 14 6 61 53 45 37 29
• 21 13 5 28 20 12 4

37

History of DES (Wikipedia)

- The origins of DES go back to the early 1970s.
- In 1972, after concluding a study on the US government's computer security needs, the US standards body NBS (National Bureau of Standards)—now named NIST (National Institute of Standards and Technology)—identified a need for a government-wide standard for encrypting unclassified, sensitive information.
- Accordingly, on 15 May 1973, after consulting with the NSA, NBS solicited proposals for a cipher that would meet rigorous design criteria. None of the submissions, however, turned out to be suitable.

40

DES Key Schedule

- The output of this permutation, called PC-1 in the literature, is divided into a 28-bit left half C_0 and a 28-bit right half D_0 . Now for each round we compute
- $C_i = C_{i-1} \ll p_i$
- $D_i = D_{i-1} \ll p_i$
- where $x \ll p_i$ means perform a cyclic shift on x to the left by p_i positions.
- If the round number i is 1, 2, 9 or 16, we shift left by one position, otherwise we shift left by two positions.

38

History of DES (Wikipedia)

- A second request was issued on 27 August 1974.
- This time, IBM submitted a candidate which was deemed acceptable—a cipher developed during the period 1973–1974 based on an earlier algorithm, Horst Feistel's Lucifer cipher.
- The team at IBM involved in cipher design and analysis included Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, and Bryant Tuckerman.

41

DES Key Schedule (PC-2)

- Finally the two portions C_i and D_i are joined back together and are subject to another permutation, called PC-2, to produce the final 48-bit round key.
- The permutation PC-2 is described to the right.

• 14 17 11 24 1 5
• 3 28 15 6 21 10
• 23 19 12 4 26 8
• 16 7 27 20 13 2
• 41 52 31 37 47 55
• 30 40 51 45 33 48
• 44 49 39 56 34 53
• 46 42 50 36 29 32

39

NSA's Involvement in the Design (Wikipedia)

- On 17 March 1975, the proposed DES was published in the Federal Register.
- Public comments were requested, and in the following year two open workshops were held to discuss the proposed standard.
- There was some criticism from various parties, including from public-key cryptography pioneers Martin Hellman and Whitfield Diffie,[1] citing a shortened key length and the mysterious "S-boxes" as evidence of improper interference from the NSA.
- The suspicion was that the algorithm had been covertly weakened by the intelligence agency so that they—but no-one else—could easily read encrypted messages

42

NSA's Involvement in the Design (Wikipedia)

- Alan Konheim (one of the designers of DES) commented, "We sent the S-boxes off to Washington.
- They came back and were all different."
- The United States Senate Select Committee on Intelligence reviewed the NSA's actions to determine whether there had been any improper involvement.
- In the unclassified summary of their findings, published in 1978, the Committee wrote: In the development of DES, NSA convinced IBM that a reduced key size was sufficient; indirectly assisted in the development of the S-box structures; and certified that the final DES algorithm was, to the best of their knowledge, free from any statistical or mathematical weakness.

43

NSA's Involvement in the Design (Wikipedia)

- and
- *NSA worked closely with IBM to strengthen the algorithm against all except brute-force attacks and to strengthen substitution tables, called S-boxes.*
- *Conversely, NSA tried to convince IBM to reduce the length of the key from 64 to 48 bits.*
- *Ultimately they compromised on a 56-bit key.*

46

NSA's Involvement in the Design (Wikipedia)

- However, it also found that NSA did not tamper with the design of the algorithm in any way.
- IBM invented and designed the algorithm, made all pertinent decisions regarding it, and concurred that the agreed upon key size was more than adequate for all commercial applications for which the DES was intended.
- Another member of the DES team, Walter Tuchman, stated "We developed the DES algorithm entirely within IBM using IBMers. The NSA did not dictate a single wire!"

44

NSA's Involvement in the Design

- Some of the suspicions about hidden weaknesses in the S-boxes were allayed in 1990, with the independent discovery and open publication by Eli Biham and Adi Shamir of differential cryptanalysis, a general method for breaking block ciphers.
- The S-boxes of DES were much more resistant to the attack than if they had been chosen at random, strongly suggesting that IBM knew about the technique in the 1970s.
- This was indeed the case; in 1994, Don Coppersmith published some of the original design criteria for the S-boxes.
- According to Steven Levy, IBM Watson researchers discovered differential cryptanalytic attacks in 1974 and were asked by the NSA to keep the technique secret.

47

NSA's Involvement in the Design (Wikipedia)

- In contrast, a declassified NSA book on cryptologic history states: *In 1973 NBS solicited private industry for a data encryption standard (DES).*
- *The first offerings were disappointing, so NSA began working on its own algorithm.*
- *Then Howard Rosenblum, deputy director for research and engineering, discovered that Walter Tuchman of IBM was working on a modification to Lucifer for general use.*
- *NSA gave Tuchman a clearance and brought him in to work jointly with the Agency on his Lucifer modification."*

45

NSA's Involvement in the Design (Wikipedia)

- Coppersmith explains IBM's secrecy decision by saying, *"that was because differential cryptanalysis can be a very powerful tool, used against many schemes, and there was concern that such information in the public domain could adversely affect national security."* Levy quotes Walter Tuchman:
- *"they asked us to stamp all our documents confidential... We actually put a number on each one and locked them up in safes, because they were considered U.S. government classified. They said do it. So I did it".*
- Bruce Schneier observed that *"It took the academic community two decades to figure out that the NSA 'tweaks' actually improved the security of DES."*

48

NSA's Involvement in the Design (Wikipedia)

- The DES can be said to have "jump-started" the nonmilitary study and development of encryption algorithms.
- In the 1970s there were very few cryptographers, except for those in military or intelligence organizations, and little academic study of cryptography.
- There are now many active academic cryptologists, mathematics departments with strong programs in cryptography, and commercial information security companies and consultants.

$$\mathbb{F}_{2^8}$$

- Recall that elements of \mathbb{F}_{2^8} are stored as bit vectors (or bytes) representing binary polynomials.
- For example the byte given by 0x83 in hexadecimal, gives the bit pattern 1, 0, 0, 0, 0, 0, 1, 1 since $0x83 = 8 \cdot 16 + 3 = 131$ in decimal.
- One can obtain the bit pattern directly by noticing that 8 in binary is 1, 0, 0, 0 and 3 in 4-bit binary is 0, 0, 1, 1 and one simply concatenates these two bit strings together.
- The bit pattern itself then corresponds to the binary polynomial $x^7 + x + 1$.
- So we say that the hexadecimal number 0x83 represents the binary polynomial $x^7 + x + 1$.
- Arithmetic in \mathbb{F}_{2^8} is performed using polynomial arithmetic modulo the irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$.
- Rijndael identifies 32-bit words with polynomials in $\mathbb{F}_{2^8}[X]$ of degree less than four.

NSA's Involvement in the Design (Wikipedia)

- A generation of cryptanalysts has cut its teeth analyzing (that is, trying to "crack") the DES algorithm.
- In the words of cryptographer Bruce Schneier, "*DES did more to galvanize the field of cryptanalysis than anything else. Now there was an algorithm to study.*"
- An astonishing share of the open literature in cryptography in the 1970s and 1980s dealt with the DES, and the DES is the standard against which every symmetric key algorithm since has been compared.

Rijndael and \mathbb{F}_{2^8}

- Rijndael identifies 32-bit words with polynomials in $\mathbb{F}_{2^8}[X]$ of degree less than four (each coefficient is an 8-bit vector)
- This is done in a big-endian format, in that the smallest index corresponds to the least important coefficient.
- Hence, the word $a_0|a_1|a_2|a_3$ will correspond to the polynomial $a_3X^3 + a_2X^2 + a_1X + a_0$.
- Arithmetic is performed on polynomials in $\mathbb{F}_{2^8}[X]$ modulo the reducible polynomial $M(X) = X^4 + 1$.
- Hence, arithmetic is done on these polynomials in a ring rather than a field, since $M(X)$ is reducible.

Rijndael

- The AES winner was decided in fall 2000 to be the Rijndael algorithm designed by Daemen and Rijmen.
- Rijndael is a block cipher which does not rely on the basic design of the Feistel cipher.
- However, Rijndael does have a number of similarities with DES. It uses a repeated number of rounds to obtain security and each round consists of substitutions and permutations, plus a key addition phase.
- Rijndael in addition has a strong mathematical structure, as most of its operations are based on arithmetic in the field \mathbb{F}_{2^8} .
- However, unlike DES the encryption and decryption operations are distinct.

AES (Wikipedia)

- The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
- AES is a subset of the Rijndael block cipher developed by two Belgian cryptographers, Vincent Rijmen and Joan Daemen, who submitted a proposal to NIST during the AES selection process.
- Rijndael is a family of ciphers with different key and block sizes.
- For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits.
- AES has been adopted by the U.S. government and is now used worldwide.
- The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data.

AES (Wikipedia)

- In the United States, AES was announced by the NIST as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001.
- This announcement followed a five-year standardization process in which fifteen competing designs were presented and evaluated, before the Rijndael cipher was selected as the most suitable.
- AES became effective as a federal government standard on May 26, 2002, after approval by the Secretary of Commerce. AES is included in the ISO/IEC 18033-3 standard.
- AES is available in many different encryption packages, and is the first (and only) publicly accessible cipher approved by the National Security Agency (NSA) for top secret information when used in an NSA approved cryptographic module (see Security of AES, below).

55

AES (Wikipedia)

- The key size used for an AES cipher specifies the number of transformation rounds that convert the input, called the plaintext, into the final output, called the ciphertext.
- The number of rounds are as follows:
 - 10 rounds for 128-bit keys.
 - 12 rounds for 192-bit keys.
 - 14 rounds for 256-bit keys.
- Each round consists of several processing steps, including one that depends on the encryption key itself.
- A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

58

AES (Wikipedia)

- AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.
- Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
- By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits.
- AES operates on a 4 × 4 column-major order array of bytes, termed the state.
- Most AES calculations are done in a particular finite field.

56

AES – High Level View (Wikipedia)

1. KeyExpansion—round keys are derived from the cipher key using Rijndael’s keyschedule. AES requires a separate 128-bit round key block for each round plus one more.
2. Initial round key addition:
 1. AddRoundKey—each byte of the state is combined with a block of the round key using bitwise xor.
3. 9, 11 or 13 rounds:
 1. SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
 2. ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
 3. MixColumns—a linear mixing operation which operates on the columns of the state, combining the four bytes in each column.
 4. AddRoundKey
4. Final round (making 10, 12 or 14 rounds in total):
 1. SubBytes
 2. ShiftRows
 3. AddRoundKey

59

AES (Wikipedia)

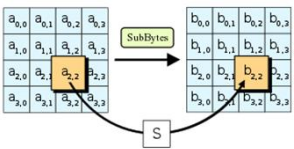
- For instance, if there are 16 bytes, b_0, b_1, \dots, b_{15} , these bytes are represented as this two-dimensional array:

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix}$$

57

The SubBytes Step

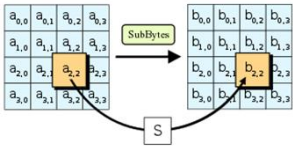
- In the SubBytes step, each byte $a_{i,j}$ in the state array is replaced with a SubByte $S(a_{i,j})$ using an 8-bit substitution box.
- This operation provides the non-linearity in the cipher.
- The S-box used is derived from the multiplicative inverse over $GF(2^8)$, known to have good non-linearity properties.



60

The SubBytes Step

- To avoid attacks based on simple algebraic properties, the S-box is constructed by combining the inverse function with an invertible affine transformation.
- The S-box is also chosen to avoid any fixed points (and so is a derangement), i.e., $S(a_i) \neq a_i$ and also any opposite fixed points, i.e., $S(a_i) \oplus a_i \neq FF_{16}$.
- While performing the decryption, the InvSubBytes step (the inverse of SubBytes) is used, which requires first taking the inverse of the affine transformation and then finding the multiplicative inverse.



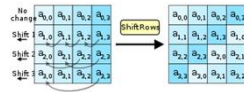
The MixColumns Step

- Matrix multiplication is composed of multiplication and addition of the entries.
- Entries are 8-bit bytes treated as coefficients of polynomial of order X^7 .
- Addition is simply XOR. Multiplication is modulo irreducible polynomial $X^8 + X^4 + X^3 + X + 1$.
- If processed bit by bit, then, after shifting, a conditional XOR with $1B_{16}$ should be performed if the shifted value is larger than FF_{16} (overflow must be corrected by subtraction of generating polynomial).
- These are special cases of the usual multiplication in $GF(2^8)$.

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \quad 0 \leq j \leq 3$$

The ShiftRows Step

- The ShiftRows step operates on the rows of the state: it cyclically shifts the bytes in each row by a certain offset.
- For AES, the first row is left unchanged.
- Each byte of the second row is shifted one to the left.
- Similarly, the third and fourth rows are shifted by offsets of two and three respectively.
- In this way, each column of the output state of the ShiftRows step is composed of bytes from each column of the input state.
- The importance of this step is to avoid the columns being encrypted independently, in which case AES degenerates into four independent block ciphers.



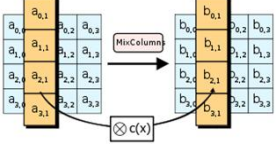
The MixColumns Step

- In more general sense, each column is treated as a polynomial over $GF(2^8)$ and is then multiplied modulo $01_{16}z^4 + 01_{16}z^3 + 01_{16}z^2 + 01_{16}z + 03_{16}$ with a fixed polynomial $c(z) = 03_{16}z^3 + 01_{16}z^2 + 01_{16}z + 02_{16}$.
- The coefficients are displayed in their hexadecimal equivalent of the binary representation of bit polynomials from $GF(2)[x]$.
- The MixColumns step can also be viewed as a multiplication by the shown particular MDS matrix in the finite field $GF(2^8)$.
- This process is described further in the article Rijndael MixColumns.

$$\begin{bmatrix} b_{0,j} \\ b_{1,j} \\ b_{2,j} \\ b_{3,j} \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} a_{0,j} \\ a_{1,j} \\ a_{2,j} \\ a_{3,j} \end{bmatrix} \quad 0 \leq j \leq 3$$

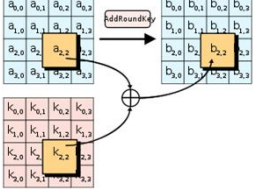
The MixColumns Step

- In the MixColumns step, the four bytes of each column of the state are combined using an invertible linear transformation.
- The MixColumns function takes four bytes as input and outputs four bytes, where each input byte affects all four output bytes.
- Together with ShiftRows, MixColumns provides diffusion in the cipher.
- During this operation, each column is transformed using a fixed matrix (matrix left-multiplied by column gives new value of column in the state):



The AddRoundKey Step

- In the AddRoundKey step, the subkey is combined with the state.
- For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state.
- The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.



Security of AES (Wikipedia)

- Until May 2009, the only successful published attacks against the full AES were side-channel attacks on some specific implementations.
- The National Security Agency (NSA) reviewed all the AES finalists, including Rijndael, and stated that all of them were secure enough for U.S. Government non-classified data.
- In June 2003, the U.S. Government announced that AES could be used to protect classified information:
- The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level.
- TOP SECRET information will require use of either the 192 or 256 key lengths.
- The implementation of AES in products intended to protect national security systems and/or information must be reviewed and certified by NSA prior to their acquisition and use.

67

Security of AES (Wikipedia)

- The authors calculate the best attack using their technique on AES with a 128 bit key requires storing 2^{80} bits of data.
- That works out to about 38 trillion terabytes of data, which is more than all the data stored on all the computers on the planet in 2016.
- As such, there are no practical implications on AES security.
- The space complexity has later been improved to 2^{56} bits, which is 9007 terabytes.
- According to the Snowden documents, the NSA is doing research on whether a cryptographic attack based on tau statistic may help to break AES.
- At present, there is no known practical attack that would allow someone without knowledge of the key to read data encrypted by AES when correctly implemented

68