Increasing security of the advanced encryption standard

Mark Lehet

Division of Science and Mathematics
University of Minnesota, Morris
Morris, Minnesota, USA

19 November 2016
Morris, MN

Why do we encrypt data?

- Encryption is a privacy-protecting technology
- Data that is important is encrypted so it cannot be read by an unintended receiver of the data
- Encryption allows for safety in data transmission

Outline

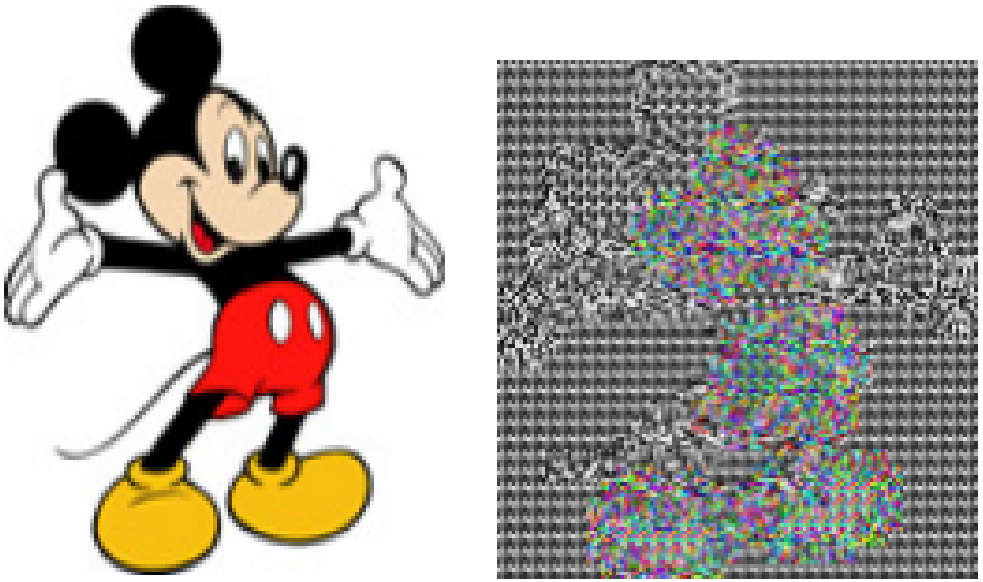
Outline

Background of AES

- Developed by two cryptographers, Joan Daemen and Vincent Rijmen
- Adopted by the National Institute of Standards and Technology in 2001
- Succeeds the former encryption standard, Data Encryption Standard

Lack of Security in AES

- Multimedia, specifically images, create a faint outline of the previous image
- Susceptible to timing attacks



a) b)

Mondal and Maitra

How AES works

AES is a symmetric key block cipher

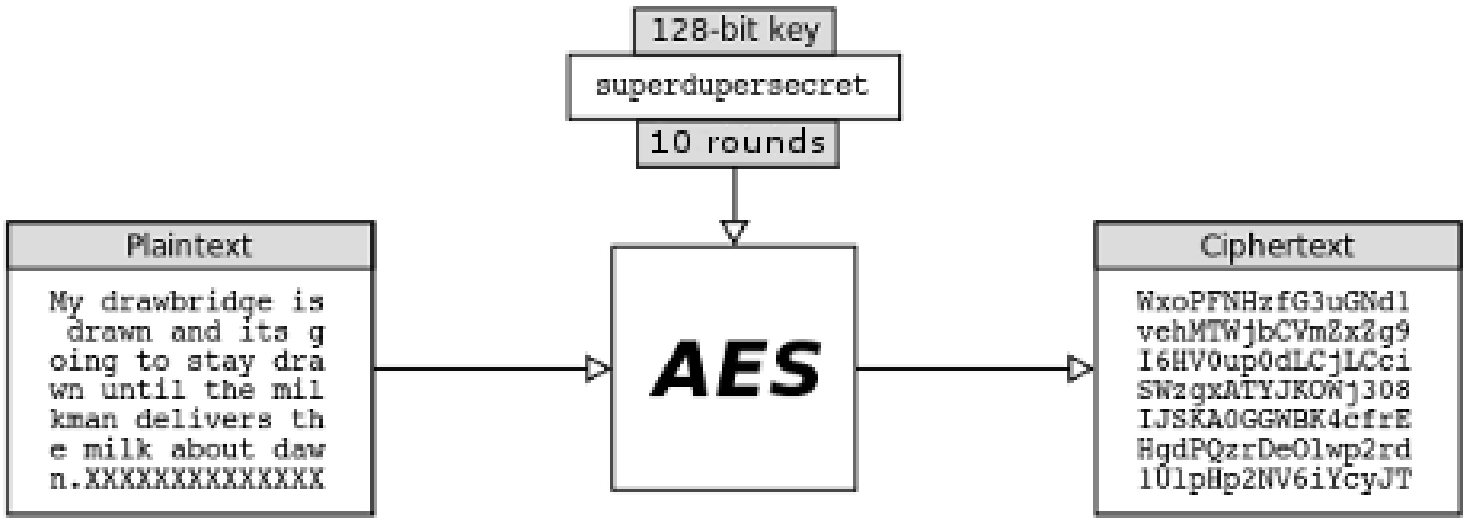
- The block size is 128 bits (16 bytes)
- The key lengths can be 128 bits, 192 bits, or 256 bits
- The block is put into a 4X4 matrix know as the state

Data that is larger than the 128 bit block size performs a mode of operation

- Pads the data to make it a multiple of 128 bits
- Splits data into multiple states
- Gives instructions on how to combine the states

How AES works

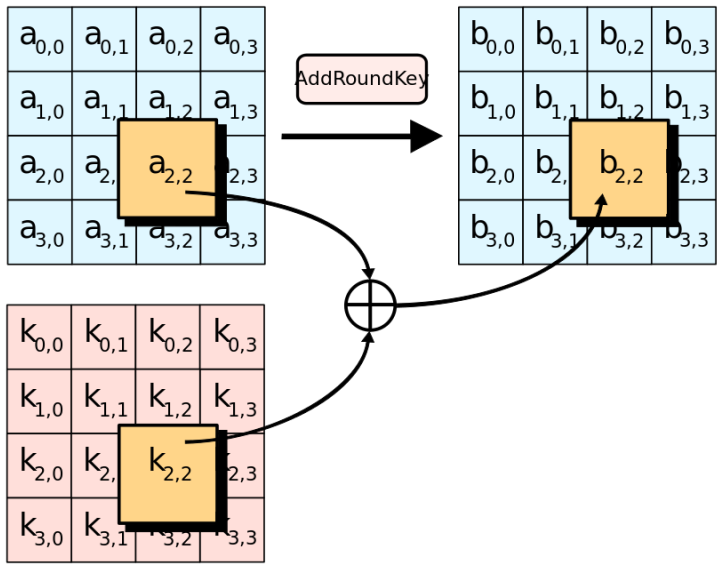
- Inputs plaintext and outputs ciphertext
- Performs certain amount of rounds depending on the key length



http://img.bityard.net/blog/aes.png

Encryption

1. KeyExpansion - generates subkeys from the initial key
2. Initial Round
   - AddRoundKey - the state is combined with the subkey derived creating a new state

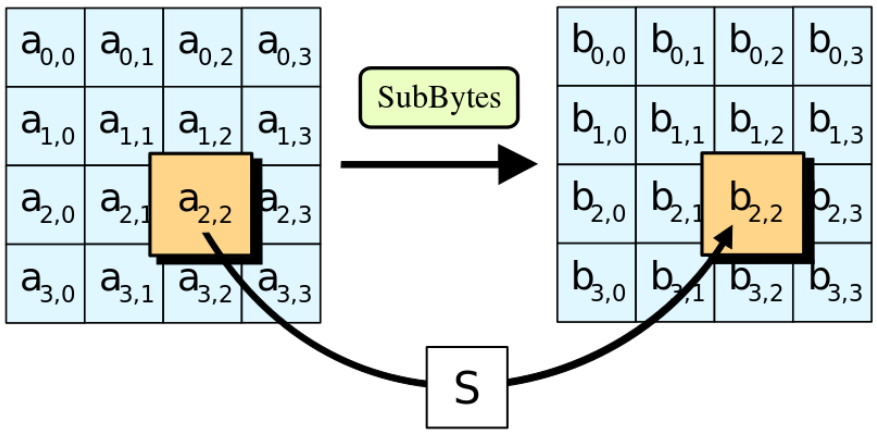


Wikipedia

Encryption

3 Rounds

- SubBytes - Each byte is substituted according to the S-Box lookup table
- S-box is generated by determining the multiplicative inverse for a given number using the finite field (2^8)

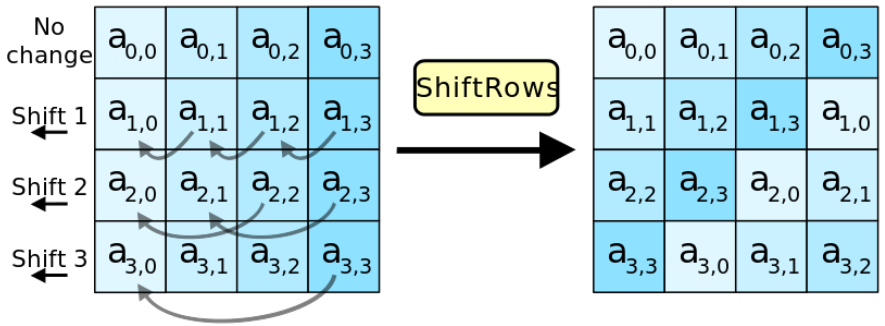


Wikipedia

Encryption

3 Rounds

- ShiftRows - Each row is cyclically shifted a certain offset

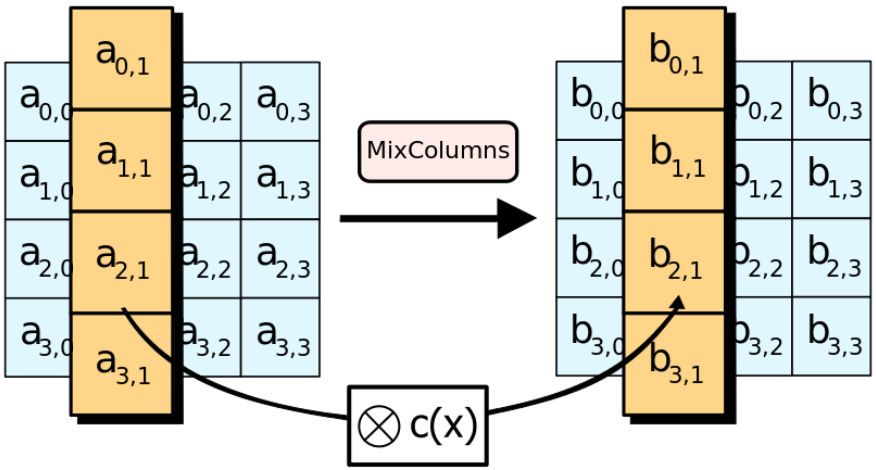


Wikipedia

Encryption

3 Rounds

- MixColumns - Each column is combined to create a new column offset



Wikipedia

Encryption

3. Rounds
   - AddRoundKey - the state is combined with the subkey derived creating a new state
4. Final Round
   - SubBytes
   - ShiftRows
   - AddRoundKey

Decryption

1. KeyExpansion (applying the keys backwards)
2. Final Round
   - AddRoundKey
   - ShiftRows
   - SubBytes
3. Rounds
   - AddRoundKey
   - MixColumns
   - ShiftRows
   - SubBytes
4. Initial Round
   - AddRoundKey

Outline

Modification

This modification aims to fix the security issue with images

- Adds a first level cipher onto the image pixels
  - Pixels on each row get offset
  - Pixels on each column get offset
- Includes randomness by generating a key from 8 random mouse positions creating a 128 bit key
- Appends the first level cipher and key to the encrypted message

Modification

1. Apply first level cipher
2. Generate random key

Uses these as the plaintext and key for AES and performs it as usual

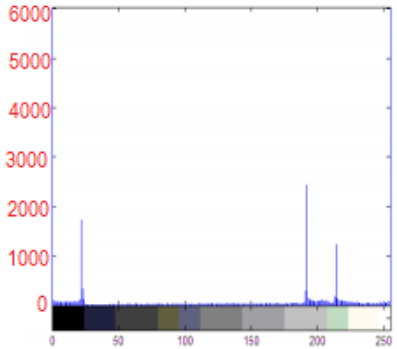
1. KeyExpansion
2. Initial Round
3. Rounds
4. Final Round
5. Appends first level cipher and key

Results

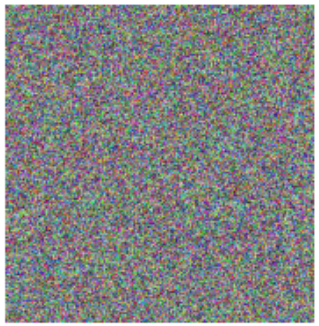
- This first level cipher adds extra security
- The randomness in the key makes it more difficult to crack

The histogram shows a more unified color tone throughout the image

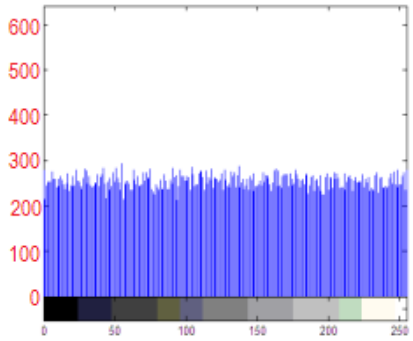
a) Original Image



b) Histogram of Original Image



c) Encrypted Image



d) Histogram of Cipher Image

Mondal and Maitra

Outline

Timing attacks

- Timing attacks fall under the category of side channel attacks
- A side channel attack attempts to gain information from the physical implementation of an algorithm
- The physical information gained from a timing attack is from the time it takes for each logical operation that is being executed on a computer
- The times gained are used to find secrets, which are used to help decrypt a ciphertext

Modification

- Developed by Behnam Rahnama, Atilla Elci, and Ibukun Eweoya

This modification aims to fix the security issue with timing attacks

An issue with AES and timing attacks is that the Final Round differs from the regular Rounds section, allowing crucial timing information to leak

- Adds the MixColumns step to the Final Round of AES
- Includes a modified playfair cipher to each round

Playfair cipher

- A playfair cipher uses a 5X5 matrix
- It takes a key and inserts it into the matrix, omitting any repeating letters
- It fills the rest of the matrix with the rest of the alphabet
- A message to be encrypted must be broken up into letter pairs, and if a pair has the same letters, they are broken up with an "X". For example, "HELLO" is broken up into "HE LX LO".

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Playfair cipher

1. If the letters are found on the same row of the matrix, you will replace the letters to their immediate right
2. If the letters are found on the same column of the matrix, you will replace the letters immediately below
3. If the letters are found on a different row or column, you would replace the letters with a letter from the same row but at the other letter pairs column

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Daniel Rodriguez-Clark

Playfair cipher

1. If the letters are found on the same row of the matrix, you will replace the letters to their immediate right

Letter Pair:
KN OW LE DG EX

Encrypted Message:
NG

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Playfair cipher

3. If the letters are found on a different row or column, you would replace the letters with a letter from the same row but at the other letter pairs column

Letter Pair:
KN OW LE DG EX

Encrypted Message:
NG RU

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Playfair cipher

2. If the letters are found on the same column of the matrix, you will replace the letters immediately below

Letter Pair:
KN OW LE DG EX

Encrypted Message:
NG RU GL

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Playfair cipher

3. If the letters are found on a different row or column, you would replace the letters with a letter from the same row but at the other letter pairs column

Letter Pair:
KN OW LE DG EX

Encrypted Message:
NG RU GL LK

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Playfair cipher

1. If the letters are found on the same row of the matrix, you will replace the letters to their immediate right

Letter Pair:
KN OW LE DG EX

Encrypted Message:
NG RU GL LK XA

E	X	A	M	P
L	B	C	D	F
G	H	I	K	N
O	Q	R	S	T
U	V	W	Y	Z

Modified Playfair Cipher

- Uses a 16X16 matrix
- Fills the matrix with ASCII character codes
- Uses the subkey used in the round as the key for the matrix
- Uses the state as the message to encrypt

Results

- The addition of the MixColumns creates consistent timing
- The modified playfair cipher strengthens security
- Time to encrypt and decrypt do increase with the modification

Outline

Conclusions

- Mondal and Maitra's modification fixes the issue of having a faint outline in an encrypted image
- The Fine Tuned AES removes the potential for timing attacks and strengthens security, but the time to encrypt and decrypt increases
- These two modifications can't be compared directly as they both address a unique security flaw with AES

Thanks!

Thank you for your time and attention!

Contact:

- lehet005@morris.umn.edu

Questions?