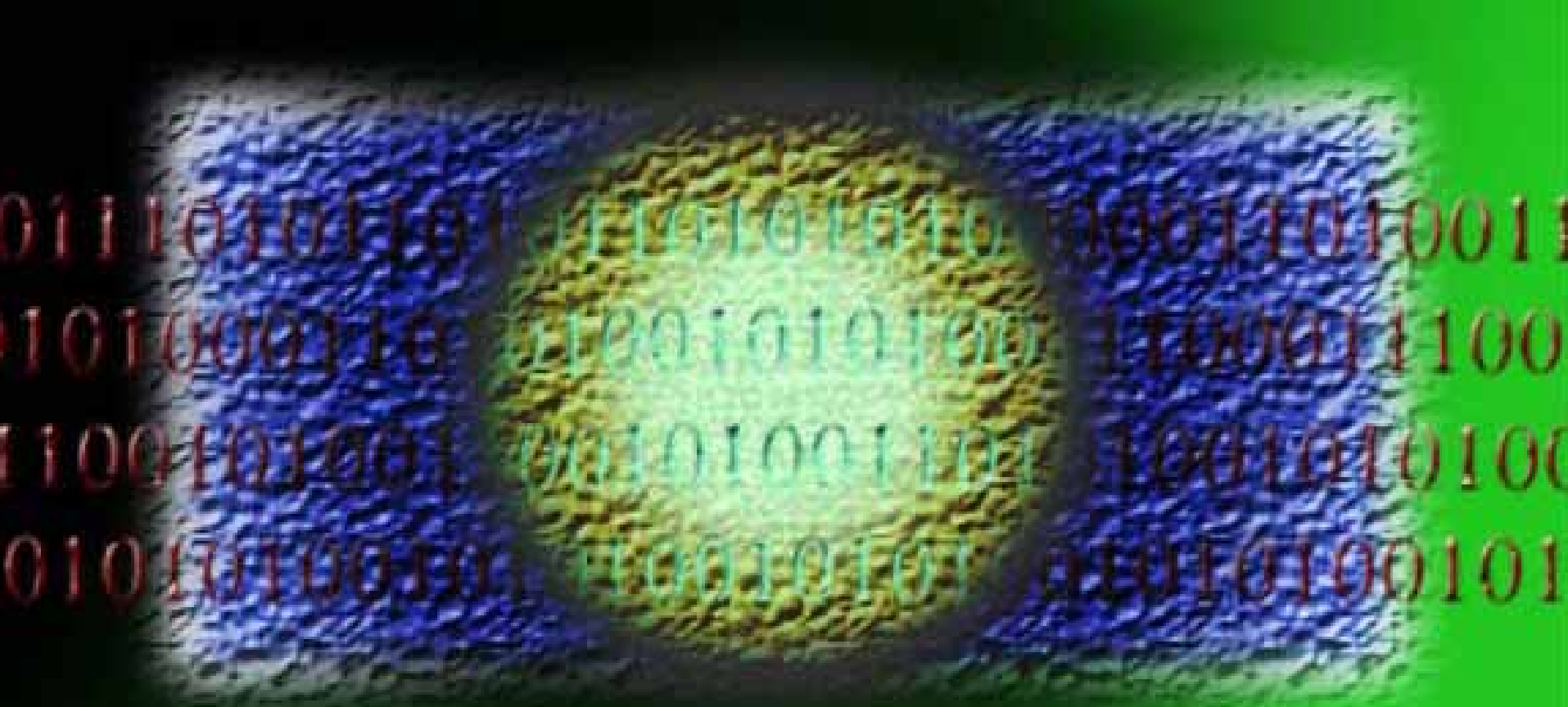


# Team ISE

## Image Selective Encryption

# Team ISE

## Image Selective Encryption


Joe Jarchow

Joseph Kadhim

Geoffrey Griffith

Shinya Daigaku

Andrew Pouzeshi

**Presentation Overview:**

- **Overview of Project**
- **Demonstration of**
  - **Manipulator**
  - **Production Code**
  - **Web Site**
- **Algorithm Design**
- **Potential Attacks**
- **Conclusion**

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Future efforts

**Problem:**

- **Multimedia files are very large**
- **Encryption is expensive**
  - **Processing time**
  - **File size**
- **No widely accepted solutions**
  - **Encrypt entire file**
  - **No encryption**

**Solution:**

**•Selective Encryption**

**Definition from MPEG paper:**

**Selective encryption applies encryption to a subset of a file with the expectation that the entire file will be rendered useless to anyone who cannot decrypt that subset.**

**Selective Encryption Requirements:**

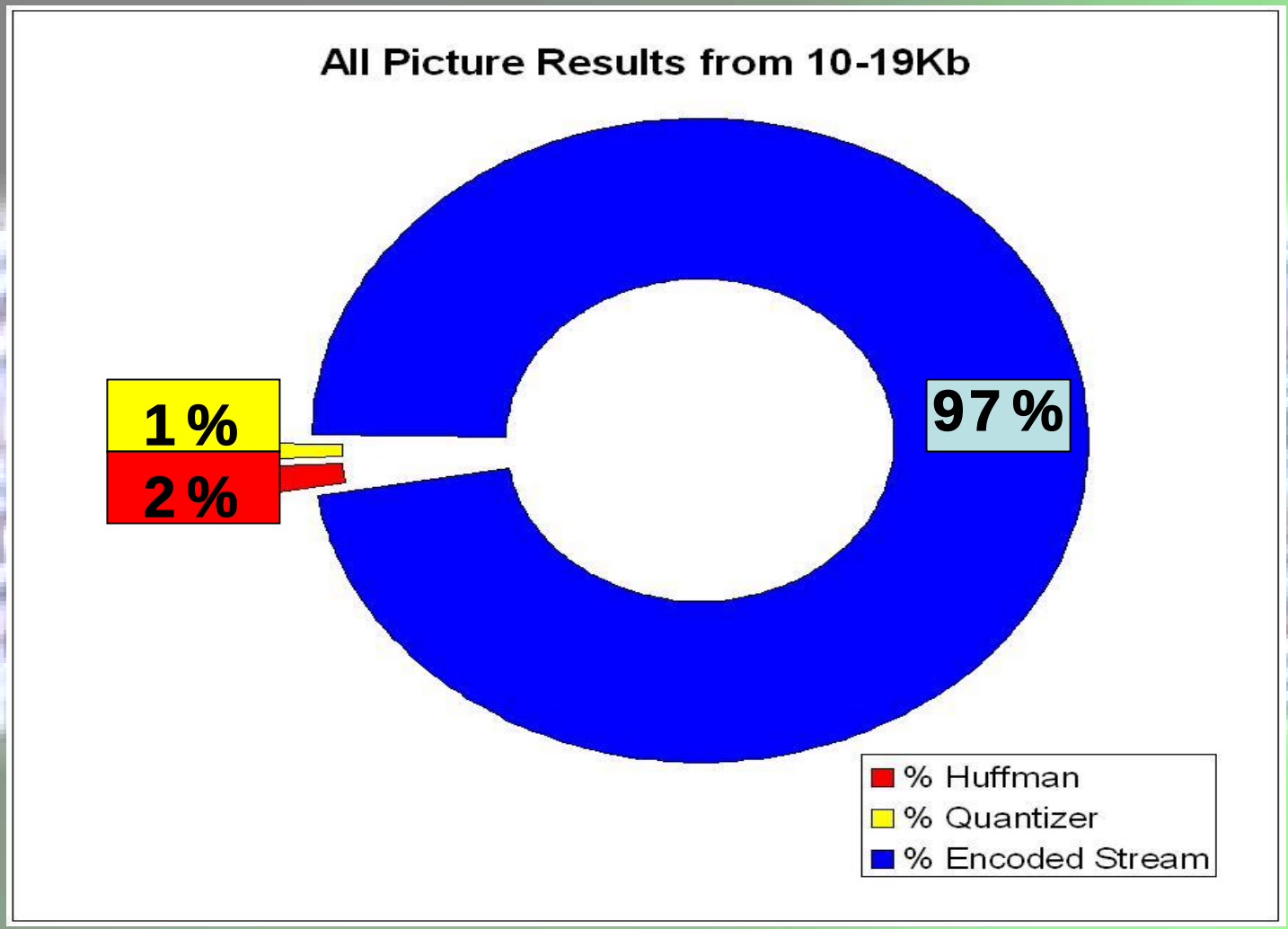
- **Perceivable degradation of file**
- **Encryption of less than 10 %**
- **Minimize required computation**
- **Minimize increase in file size**
- **Cryptanalytic approach**

**JPEG Requirements**

- **Only Baseline standard**

**Criteria For Bad Targets:**

- **Optional markers**
- **Not used in Baseline JPEG images**
- **No effect on image quality**
- **Easily guessed or forged by a hacker**


All Picture Results from 10-19Kb
1 %
2 %
97 %
% Huffman
% Quantizer
% Encoded Stream

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

**Demonstration of Manipulator:**

- **Layout vs. JPEG standard**
- **Show new features (project file, etc.)**
- **Cover earlier research**
- **Propose possible attacks**
- **Show table manipulation**
- **Show table replacement**

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

**Demonstration of Production Code:**

- **Run demonstration script**
- **During run, show code (h, cpp, scripts)**
- **Explain tests run in script (diff)**
- **Show images for comparison**
- **Show .ise will not work**

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

**Demonstration of Manipulator:**

- **Show menu bar links**
- **Show each page**
- **Show message board**
- **Show message board administration**
- **Show HTML code**
- **Plead for domain NAME!**

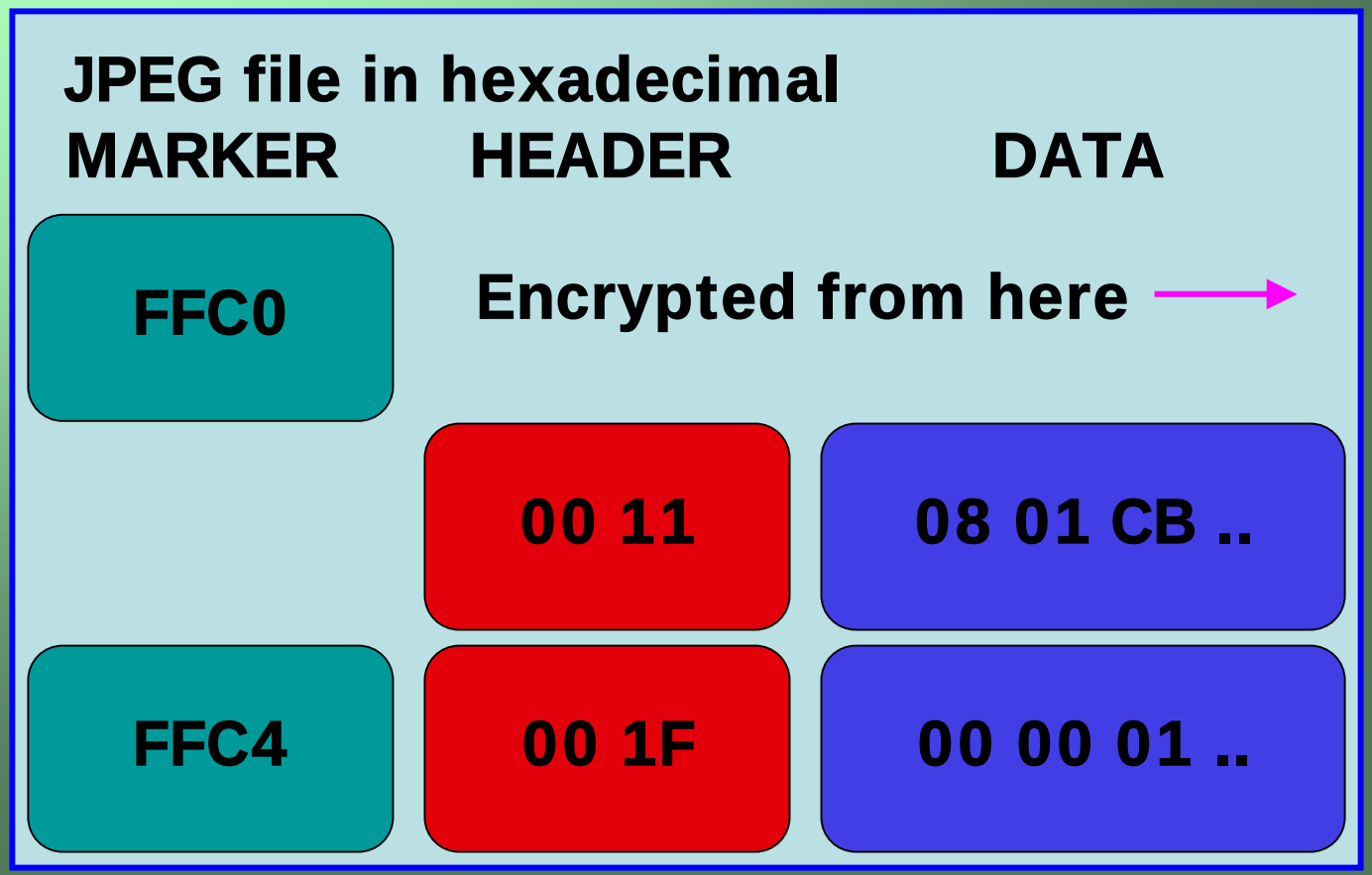
**Presentation Overview:**

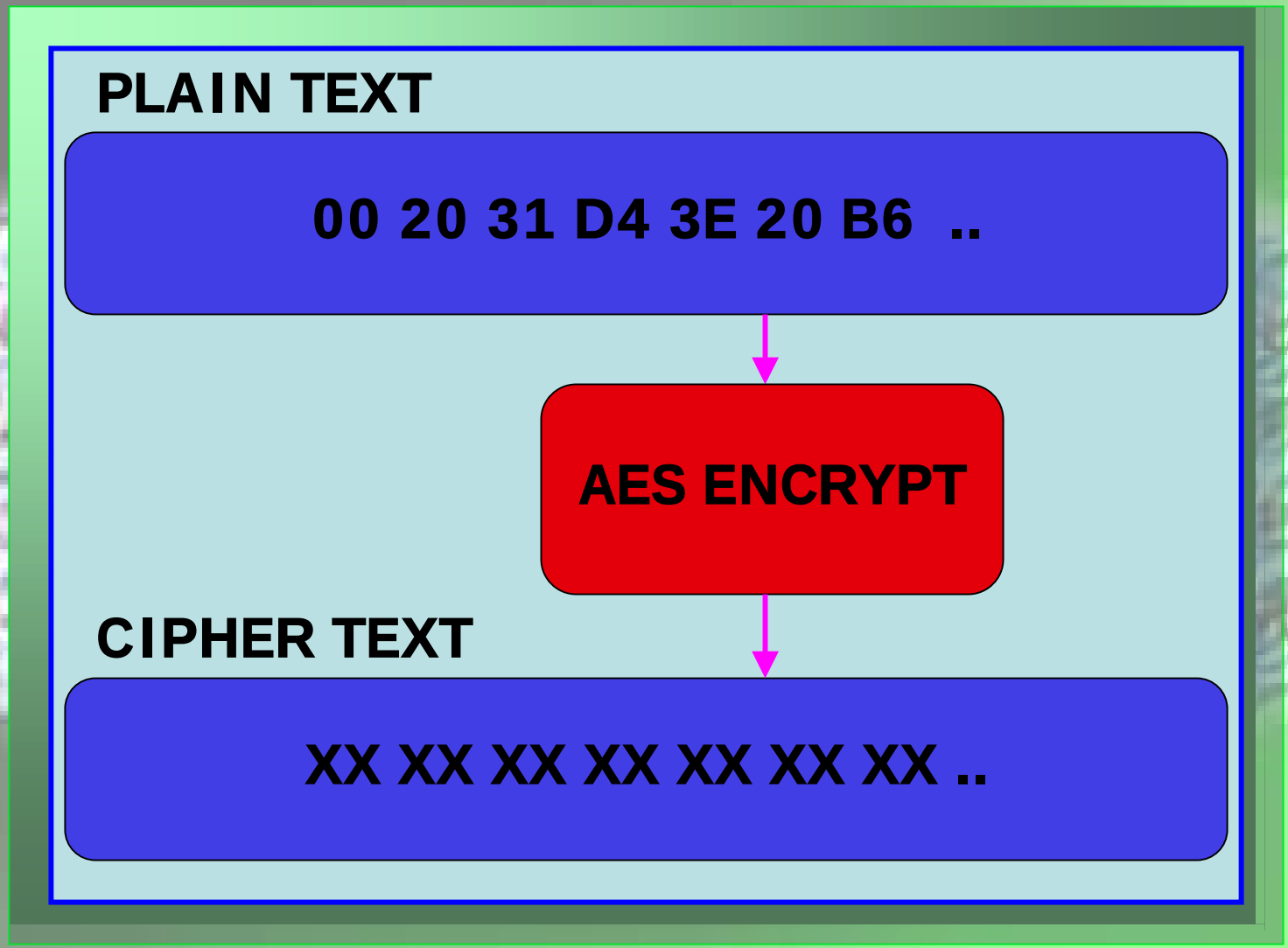
- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

**Encryption Algorithm:**

- **Write file-type-byte to ".ise" file**
  - **'1' for JPEG**
- **Read from input file**
- **Write unencrypted to ".ise" file**
- **Read/Write until Huffman**
  - **[FF C0 or FF C4]**
  - **baseline standard Huffman tables**

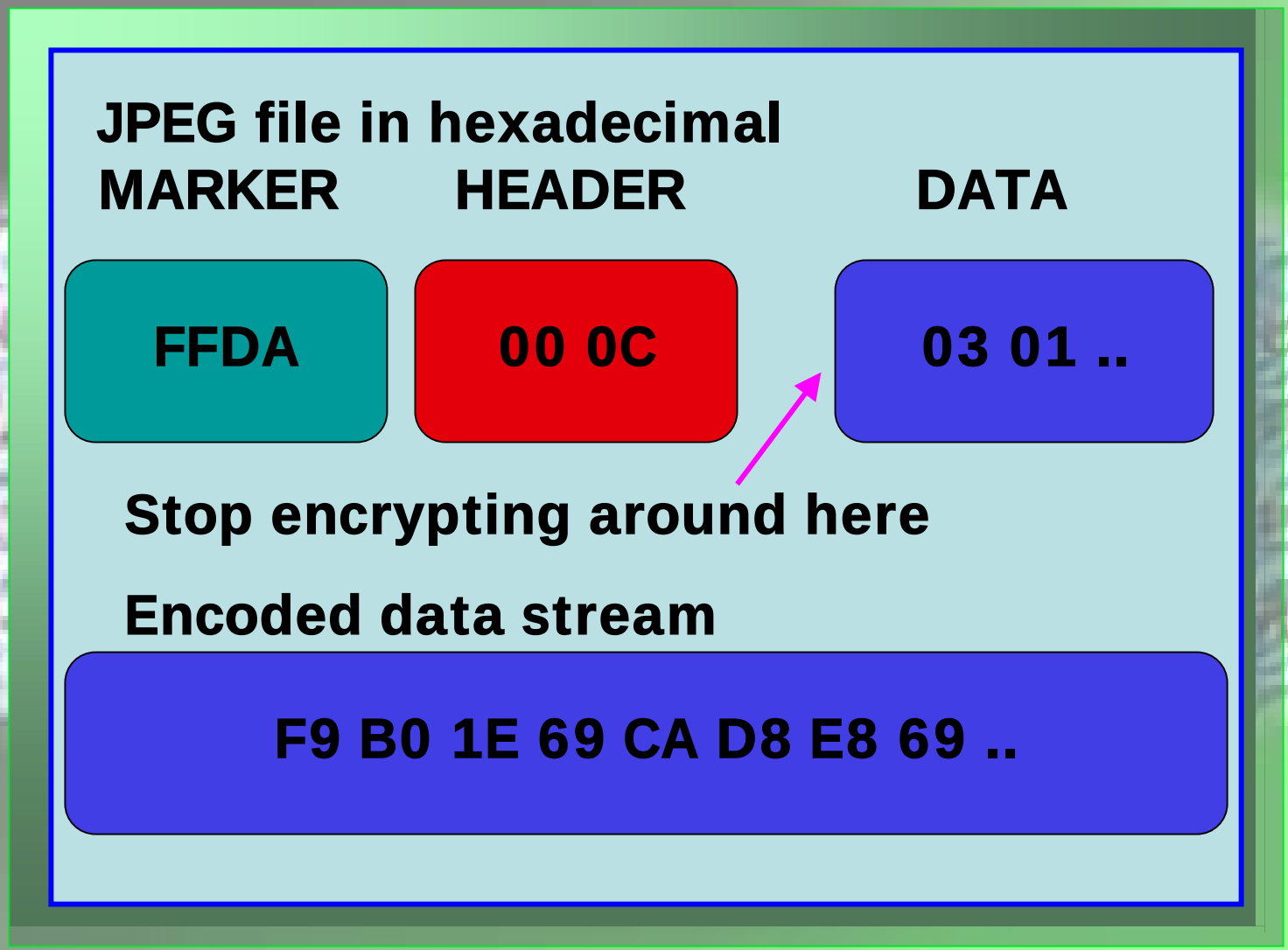
## Start Encrypting After FFC0:




PLAIN TEXT
00 20 31 D4 3E 20 B6 ..
AES ENCRYPT
CIPHER TEXT
XX XX XX XX XX XX XX ..

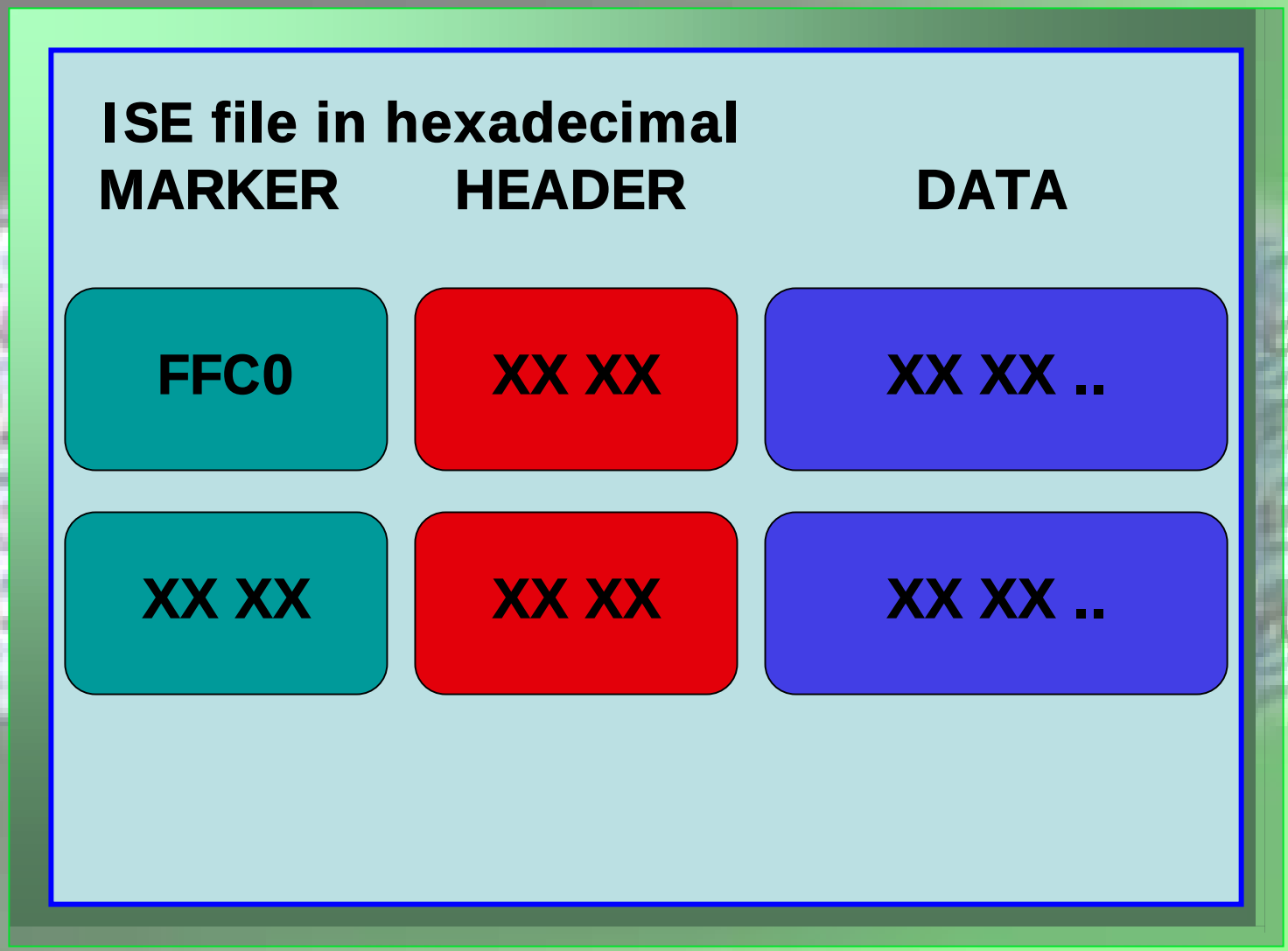
**Encryption Algorithm:**

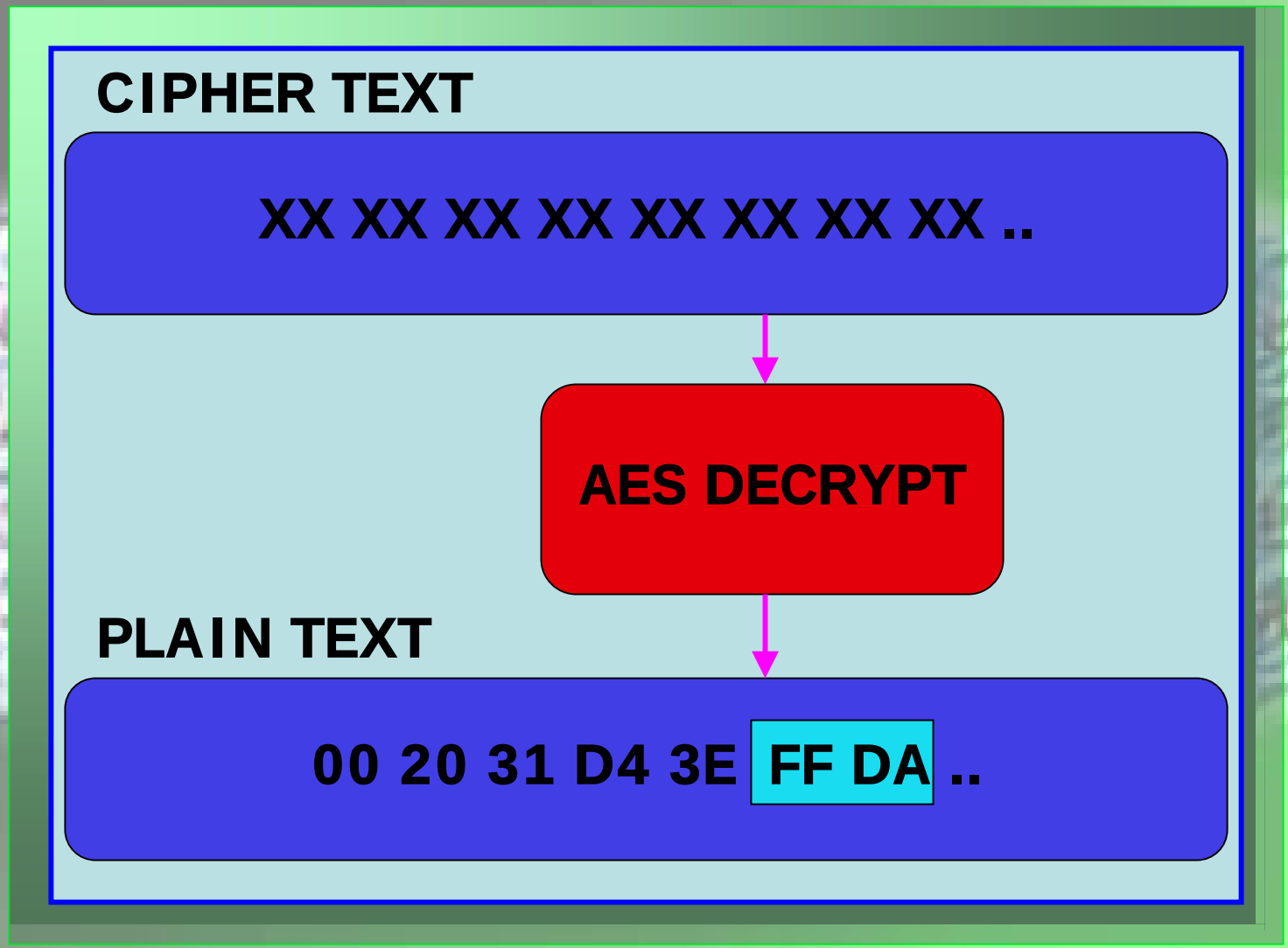
- **Keep encrypting until encoded data**
  - **[FF DA]**
  - **Start of encoded data stream**
- **Hide marker inside encrypted area**
- **Hide random length of encoded data**


JPEG file in hexadecimal
MARKER
HEADER
DATA
FFDA
00 0C
03 01 ..
Stop encrypting around here
Encoded data stream
F9 B0 1E 69 CA D8 E8 69 ..

**Decryption Algorithm:**

- **Read file-type-byte from ".ise" file**
  - **'1' for JPEG**
- **Read / Write until Huffman**
  - **[FF C0 or FFC4]**
  - **baseline standard Huffman tables**
- **Start decrypting**


ISE file in hexadecimal
MARKER
HEADER
DATA
FFC0
XX XX
XX XX ..
XX XX
XX XX
XX XX ..


CIPHER TEXT
XX XX XX XX XX XX XX XX ..
AES DECRYPT
PLAIN TEXT
00 20 31 D4 3E FF DA ..

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

**Potential Attacks:**

- **Brute force replacement**
- **Inside knowledge**
  - **Password**
  - **Image editor**
- **Could implement AES with larger**
  - **Key**
  - **Block length (further into data)**
- **Data is relatively untouched**
  - **Except at head**

**Presentation Overview:**

- Overview of Project
- Demonstration of
  - Manipulator
  - Production Code
  - Web Site
- Algorithm Design
- Potential Attacks
- Conclusion

# Questions