Cryptanalysis, Side Channel Attacks and Stream Ciphers

Dhiren Patel
(Oct 2022)

- Classical ciphers
- Weaknesses
- Hacking
- Industry requirement

Cryptanalysis

- Two general approaches to attack a conventional encryption scheme
  - Brute-force attack
    - attacker tries every possible key on a piece of ciphertext
  - Cryptanalytic attack
    - rely on the nature of the algorithm plus perhaps some knowledge of the general characteristics of the plaintext or even some sample plaintext-ciphertext pairs

Brute-force Attack

- Trying every possible key until an intelligible translation of the ciphertext into plaintext is obtained.

Key size (bits)	Number of alternative keys	Time required at 1 decryption/ms		Time required at 10^6 decryption/ms
32	$2^{32} = 4.3 \times 10^9$	2^{31} ms	= 35.8 minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	2^{55} ms	= 1142 years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	2^{127} ms	$= 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	2^{167} ms	$= 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	2×10^{26} ms	$= 6.4 \times 10^{12}$ years	6.4×10^6 years

Cryptanalytic attacks

Type of Attack	Known to Cryptanalyst
Ciphertext only	• Encryption algorithm • Ciphertext
Known Plaintext	• Encryption algorithm • Ciphertext • One or more plaintext-ciphertext pairs formed with the secret key
Chosen Plaintext	• Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

Cryptanalytic attacks

Type of Attack	Known to Cryptanalyst
Chosen Ciphertext	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	• Encryption algorithm • Ciphertext • Purported ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key

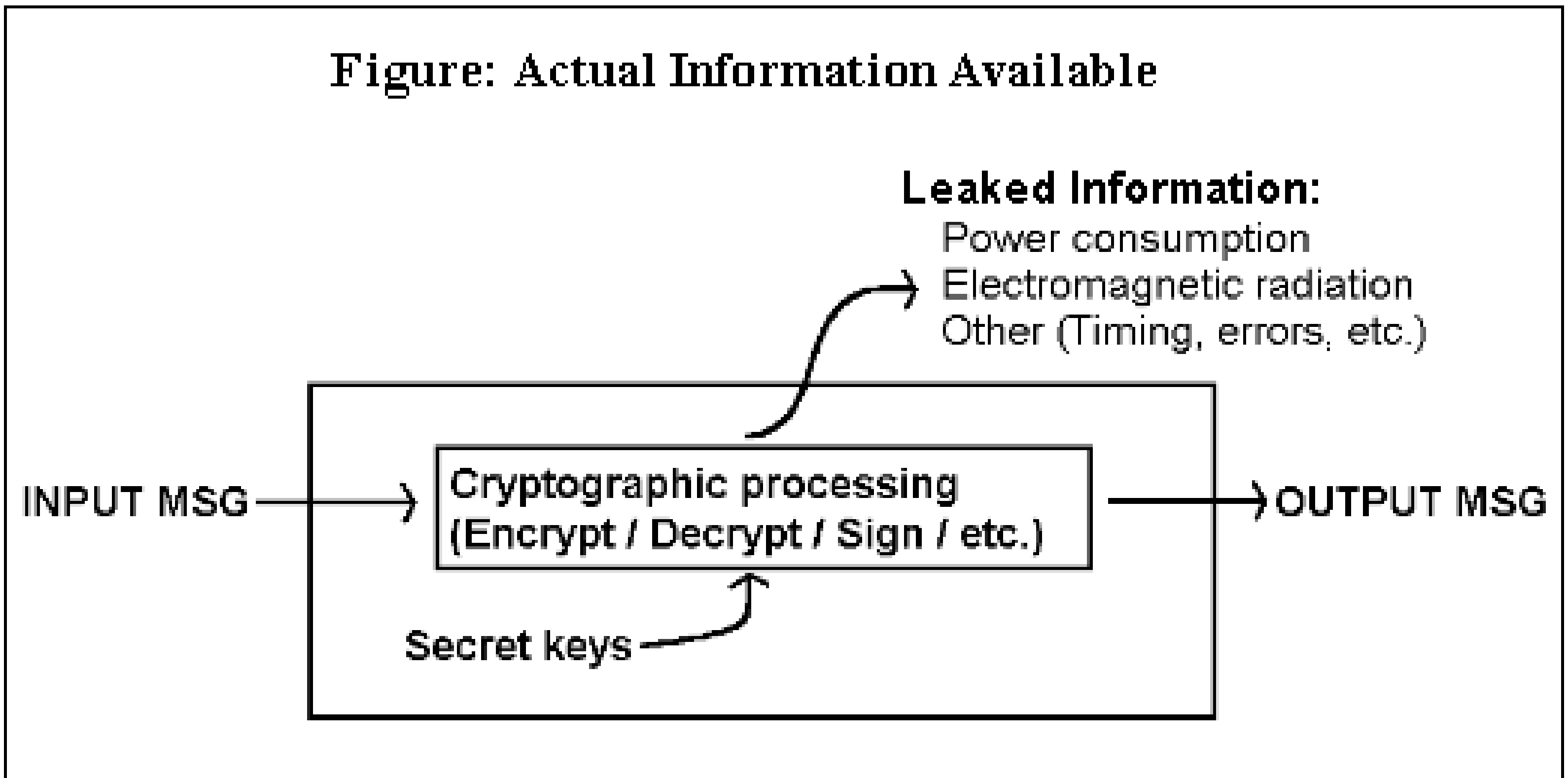
Side Channel Attacks (Cryptanalysis)

- Black box model….

Side channel attacks

- EMI – e.g. CRT, copy of tty in next room
- Traffic analysis - war zones - Military movement, optical – IR US embassy
- Timing analysis (next slide)
- Power analysis

Side channel attacks



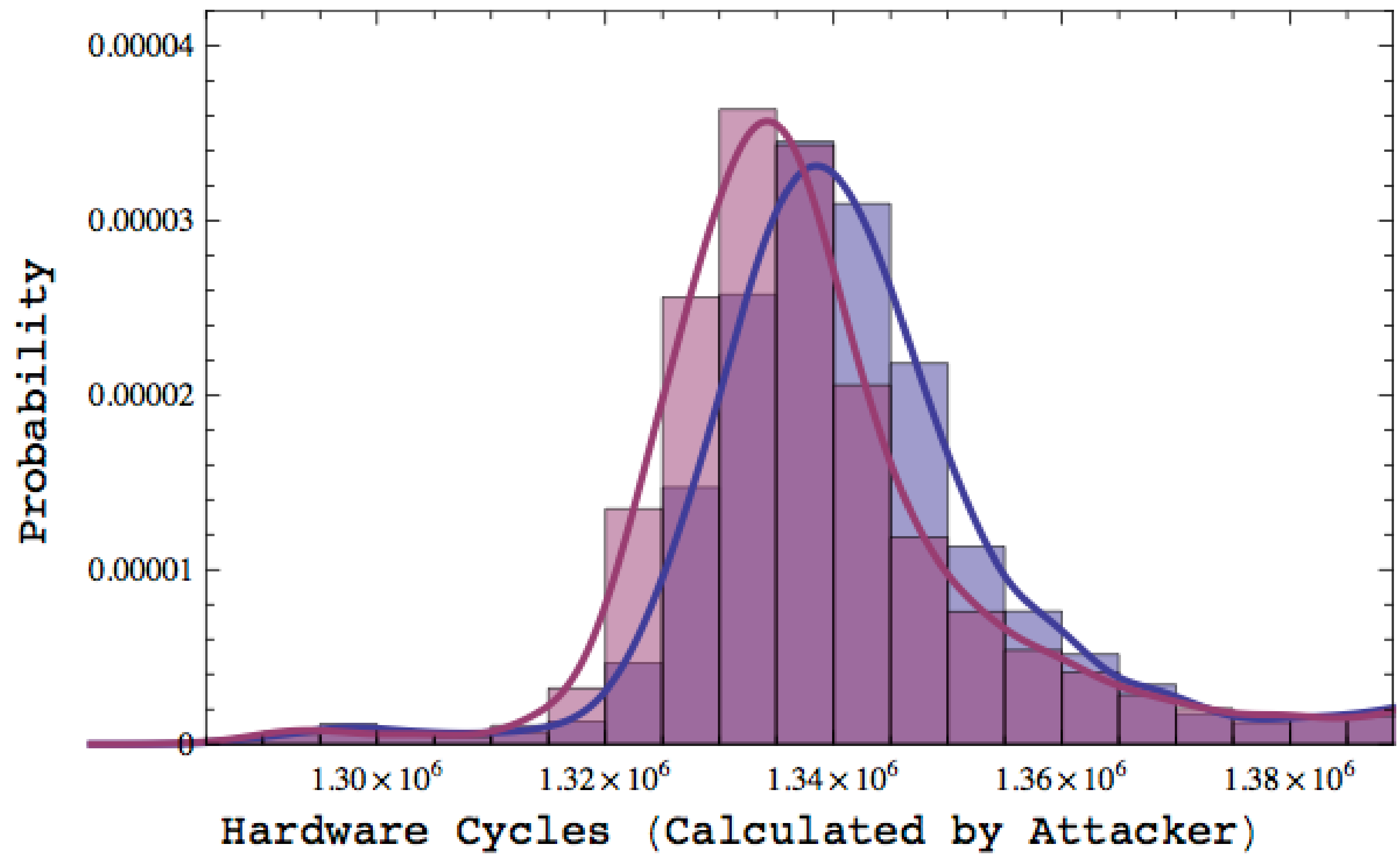
Timing attacks

- If Alice wants to secure her home, she could buy high-quality locks and install several of them on her door. However, a clever burglar might simply unscrew the hinges, remove the door and walk away with all of Alice's valuables with minimal effort.
- This example of an indirect attack on household security - there exists a parallel in the world of encryption that is quite real. It is called the timing attack and it has been used to defeat some of the most popular encryption techniques!!!

Timing attack

- Timing attacks are based on measuring how much time various computations take to perform.
- By observing variations in how long it takes to perform cryptographic operations, it can be possible to determine the entire secret key

- Timing attacks are a form of side channel attack where an attacker gains information from the implementation of a cryptosystem rather than from any inherent weakness in the mathematical properties of the system.
- Such attacks involve statistical analysis of timing measurements

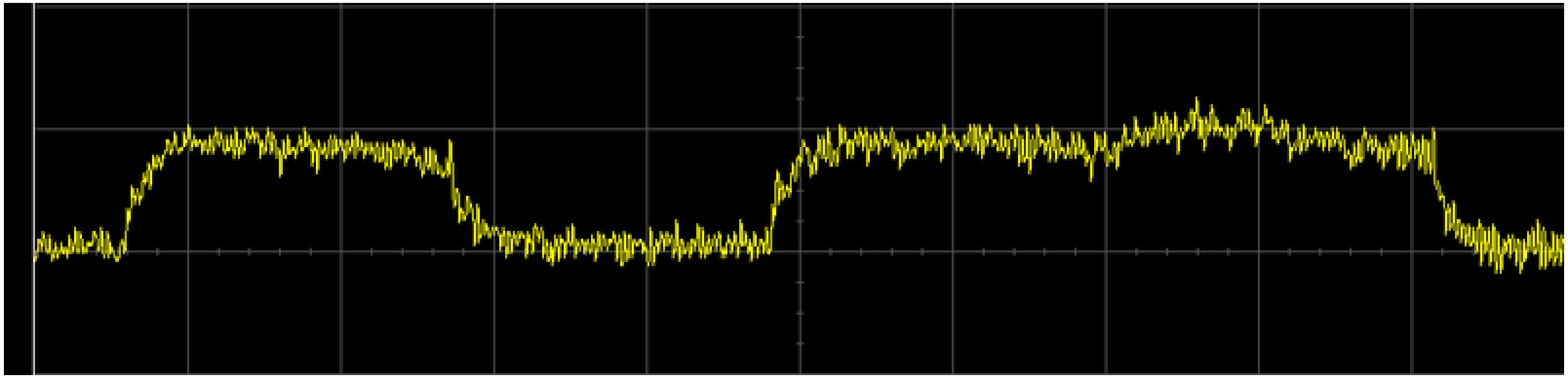

0.00004
0.00003
0.00002
0.00001
0
Probability
1.30×10^6
1.32×10^6
1.34×10^6
1.36×10^6
1.38×10^6
Hardware Cycles (Calculated by Attacker)

Countermeasures

- multiplications take a constant amount of time, independent of the size of the factors
- Montgomery algorithm
- Chinese Reminder Theorem
- Blinding

Power analysis

- by observing the power consumption of a hardware device such as CPU or cryptographic circuit



- Power variations, observed during work of the embedded processor, computing RSA signatures.
- The left (short) peak represents iteration without multiplication, and the right represents iteration with multiplication.
- The low power pause between iterations has been artificially implemented to make key decoding trivial.

- E.g. RISC/CISC – pipelining, bubble, Instruction Set Design, weak computing device (smart card)

Misc…

- In the 1980s, Soviet eavesdroppers were suspected to plant bugs inside IBM electric typewriters to monitor the **electrical noise** generated as the type ball rotated and pitched to strike the paper; the characteristics of those signals could determine which key was pressed.

Countermeasures (Side channel attacks)

- Special shielding
- JAM
- Random delay
- Instruction set design
- constant execution path

Scalable v/s Targeted attacks

- When does targeting make sense for an attacker?
- Low yield automated attacks
- Expensive – high touch social engineering attack
- Drive-by-download, self replicating,
- Physical side channel, targeted

STREAM CIPHERS

Cryptography Classification

- Cryptographic systems are characterized along three independent dimensions:

1. The type of operations used for transforming plaintext to cipher text
   - E.g. Substitution, transposition etc.
2. The type of keys used
   - Symmetric key
   - Asymmetric key (different keys for encryption/decryption)
3. The way in which the plaintext is processed
   - Block cipher
   - Stream cipher (one by one – bit/char)

Block cipher v/s. Stream cipher

- Block ciphers operate with a fixed transformation on large blocks of plaintext data;
- Stream ciphers operate with a time-varying transformation on individual plaintext digits
- E.g. Lorenz SZ-42 cipher machine, RC4, SEAL, Slasa20
- eSTREAM – ECRYPT Stream Cipher project

Stream cipher

- The system can be expressed as:

$c_i = m_i \oplus k_i$ – Encryption

$m_i = c_i \oplus k_i$ – Decryption //??

- where, $m_i = i^{th}$ binary digit of plain text
- $k_i = i^{th}$ binary digit of key material
- $c_i = i^{th}$ binary digit of cipher text
- $\oplus$ = exclusive-or (XOR) operation

- OTP – cipher text is statistically independent of plain text
- A stream cipher attempts to capture the spirit of the one-time pad by using a short key to generate the keystream which appears to be random.

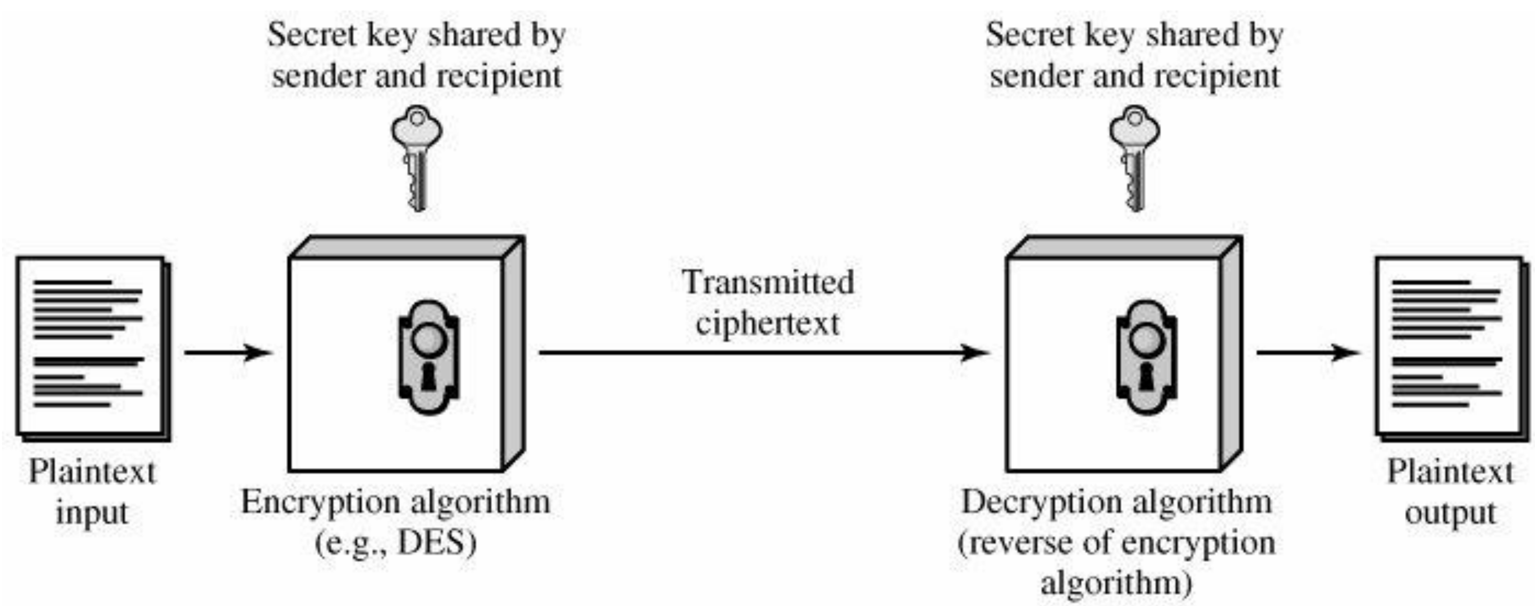
Stream cipher

- The generation of the keystream can be independent of the plaintext and ciphertext, yielding *synchronous* stream cipher,
- It can also depend on the data and its encryption, in which case the stream cipher is said to be *self-synchronizing*.
- Most stream cipher designs are for synchronous stream ciphers.

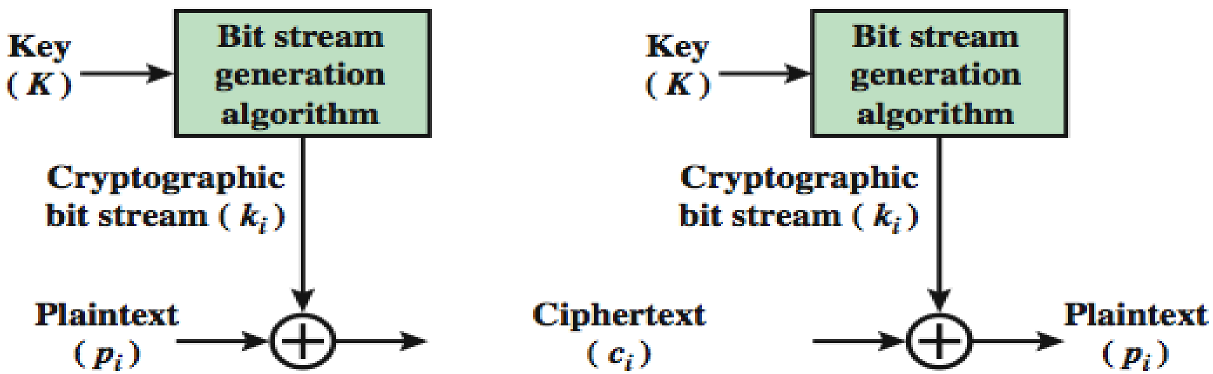
SKC Model

- A symmetric encryption scheme has five ingredients

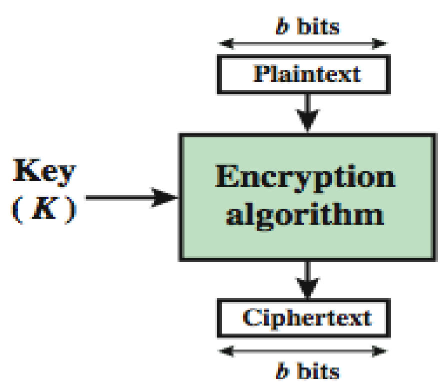
1. Plain Text
2. Encryption Algorithm
3. Secret Key
4. Cipher Text
5. Decryption Algorithm



Block Cipher vs. Stream Cipher



(a) Stream Cipher Using Algorithmic Bit Stream Generator



(b) Block Cipher

Stream cipher key generator

- Key gen Algorithm shared
- Based on seeds
- E.g. Sensex of previous day as seed next day
- <weekends no communication!!!!!>

Properties – Synchronous cipher!!

- Of more practical significance, both the encrypting and decrypting units must remain in step since decryption cannot proceed successfully unless the keystreams used to encrypt and decrypt are synchronized.
- Synchronization is usually achieved by including 'marker positions' in the transmission.

Properties – Asynchronous cipher!!

- In contrast, self-synchronizing (asynchronous) stream ciphers have the facility to resume correct decryption if the keystream generated by the decrypting unit falls out of synchronization with the encrypting keystream.
- For these stream ciphers the function that defines the next state of the cryptosystem takes as input some of the previously generated ciphertext!!

Asynchronous ciphers!!

- Suppose the encryption of a bit depends on *c* previous ciphertext bits.
- The system demonstrates limited error propagation; if one bit is received incorrectly then decryption of the following *c* bits may be incorrect.
- Additionally however, the system is able to resynchronize itself and produce a correct decryption after *c* bits have been received correctly.
- This makes such ciphers suitable for applications where synchronization is difficult to maintain.

Properties!!!

- As each plaintext bit is encrypted independently of the others and the corruption of a bit of the ciphertext during transmission will not affect the decryption of other ciphertext bits.
- The cipher is described as having no error-propagation and though this appears to be a desirable property, it has several implications.
- First, it limits the opportunity to detect an error when decryption is performed,
- Second, an attacker is able to make controlled changes to parts of the ciphertext knowing fully well what changes are being induced on the corresponding plaintext.