Cryptology for IoT

Modules M4, M6, M8
Session of 26th May, 2022.

M8.1 Briefing of the session
M8.2 Modern Cryptography
M8.3 Modern Cryptanalysis

Prof.: Guillermo Botella

Cryptology for IoT

Modules M4, M6, M8
Session of 26th May, 2022.

M8.1 Briefing of the session
M8.2 Modern Cryptography
M8.3 Modern Cryptanalysis

Prof.: Guillermo Botella

M8.1 Briefing of today

- Introducing modern Cryptography and Cryptanalysis
- Stream Ciphers and Block ciphers
  - Slides and supplementary videos
  - Practice using Cryptool
- Entropy Cryptanalysis
  - Slides and supplementary videos
  - Practice using Cryptool
- We will go to the Socrative.
  - (continuation of the previous quiz)

Cryptology for IoT

Modules M4, M6, M8
Session of 26th May, 2022.

M8.1 Briefing of the session
M8.2 Modern Cryptography
M8.3 Modern Cryptanalysis

Prof.: Guillermo Botella

Modern Cryptography

Modern Ciphers – Basic Terms

Modern Symmetric Ciphers

Modern Asymmetric Ciphers

Federal Information
Processing Standards Publication 197

November 26, 2001

Announcing the

ADVANCED ENCRYPTION STANDARD (AES)

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. **Name of Standard.** Advanced Encryption Standard (AES) (FIPS PUB 197).
2. **Category of Standard.** Computer Security Standard, Cryptographic.
3. **Explanation.** The Advanced Encryption Standard (AES) specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

4. **Approving Authority.** Secretary of Commerce.
5. **Maintenance Agency.** Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).
6. **Applicability.** This standard may be used by Federal departments and agencies when an agency determines that sensitive (unclassified) information (as defined in P. L. 100-235) requires cryptographic protection.

Other FIPS-approved cryptographic algorithms may be used in addition to, or in lieu of, this standard. Federal agencies or departments that use cryptographic devices for protecting classified information can use those devices for protecting sensitive (unclassified) information in lieu of this standard.

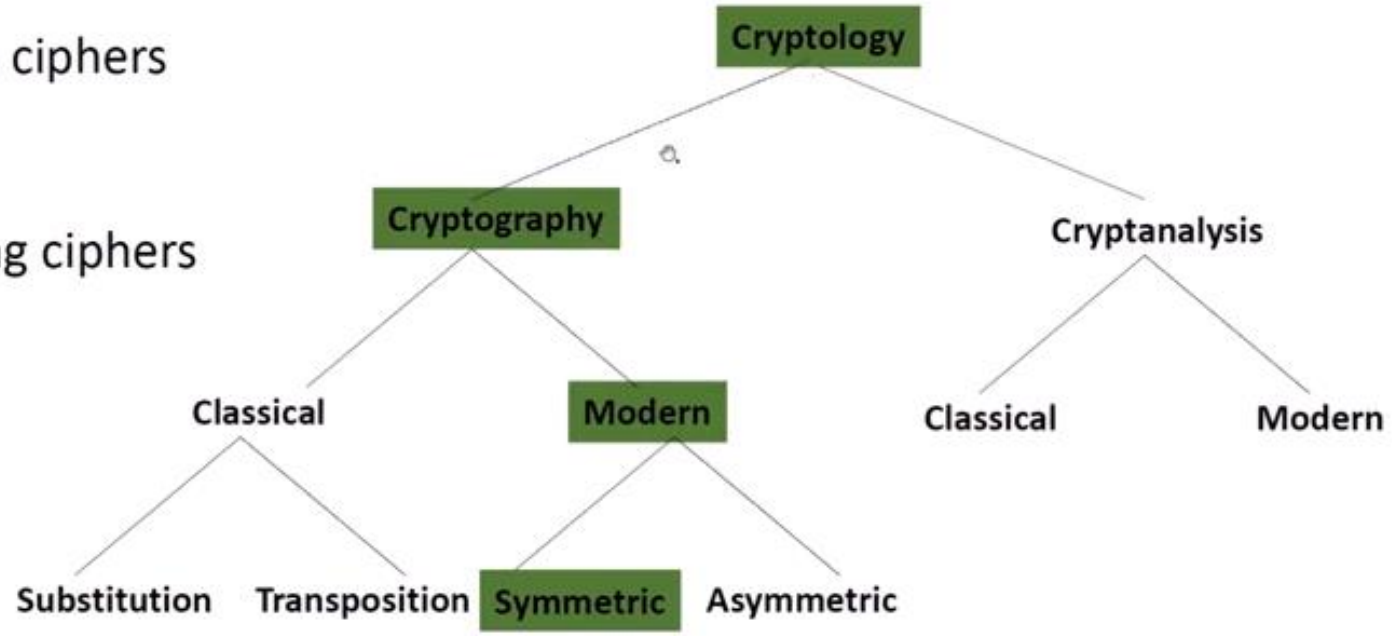
In addition, this standard may be adopted and used by non-Federal Government organizations. Such use is encouraged when it provides the desired security for commercial and private organizations.

Federal Information Processing Standards Publication 197
ADVENCED ENCRYPTION STANDARD (AES), 2001

Modern Cryptography

Cryptography
Art of making ciphers

Cryptanalysis
Art of breaking ciphers



Modern Cryptography

Modern cipher

- Computer-based encryption algorithm; works on binary data

Plaintext alphabet

- Binary data, e.g. a byte (10010101)

Ciphertext alphabet

- Binary data, e.g. a byte (00110011)

Key

- Binary data, e.g. a byte (00111001)

Key length / key size

- Given in bit, for example DES 56bit, AES 128bit, or RSA 2048bit
- A minimum of 128bit/2048bit (symmetric/asymmetric) is considered to be secure

Modern Cryptography

Symmetric cipher

- Uses the same key *K* for encryption and decryption
- Examples: DES, AES, RC5, Camelia, Blowfish

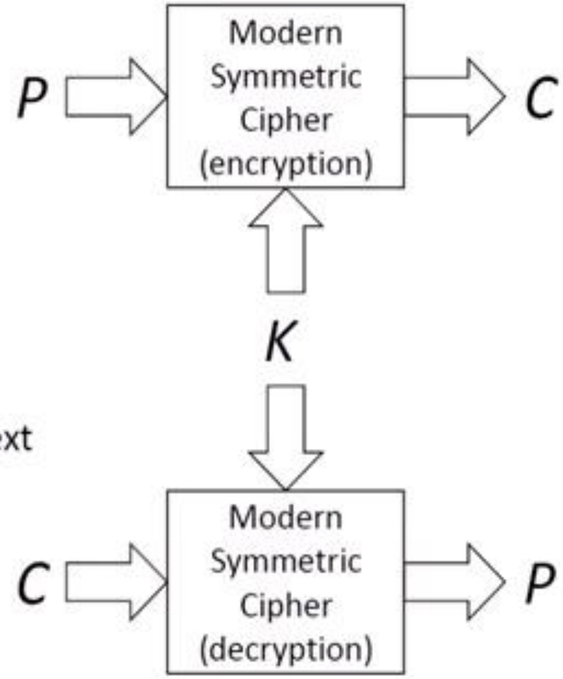
Asymmetric cipher

- Uses two different keys *E* and *D* for encryption and decryption
- Examples: RSA, Paillier

Some important requirements on modern ciphers

- Change of only a single one bit in input should change on average 50% of the output bits
- Have to be secure with respect to each type of attack (chosen-plaintext, known-plaintext, ciphertext-only)
- Considered broken, if any of the aforementioned attacks is found

Modern Cryptography



Symmetric cipher

- Uses the same key *K* for encryption and decryption
- Key *K*, Plaintext *P*, and Ciphertext *C*

Two main classes of modern symmetric ciphers

Stream ciphers

- Generate a pseudorandom keystream that is XOR-ed with the plaintext
- Even with the knowledge of parts of the keystream, the preceding and subsequent bits should not be computable by an attacker

Block ciphers

- Encrypt a block of several bits of the plaintext at the same time

Modern Cryptography

Plaintext *P*:
HELLO ...

Plaintext *P* (encoded as binary data):
01001000 01000101 01001100 01001100 01001111 ...

Keystream K_S (produced by stream cipher; based on key *K*):
10011000 01110110 10111001 10000010 00010111 ...

Ciphertext *C* encrypted by: $C = P \text{ XOR } K_S$
11010000 00110011 11110101 11001110 01011000 ...

Plaintext *P* decrypted by: $P = C \text{ XOR } K_S$
01001000 01000101 01001100 01001100 01001111 ...

Plaintext *P*:
HELLO ...

XOR	1	0
1	0	1
0	1	0

$C = P \text{ XOR } K_S$

$P = C \text{ XOR } K_S$
$= (P \text{ XOR } K_S) \text{ XOR } K_S$
$= (P \cancel{\text{ XOR } K_S) \text{ XOR } K_S}$
$= P$

Modern Cryptography

Plaintext *P*:
HELLO ...

Plaintext *P* (encoded as binary data):
01001000 01000101 01001100 01001100 01001111 ...

Ciphertext *C* encrypted by: $C = Cipher_{ENC}(P,K)$
10010101 11110010 10101101 10101101 01110011 ...

Plaintext *P* decrypted by: $P = Cipher_{DEC}(C,K)$
01001000 01000101 01001100 01001100 01001111 ...

Plaintext *P*:
HELLO ...

Remark: Same plaintext blocks are encrypted as same ciphertext blocks!

Modern Cryptography

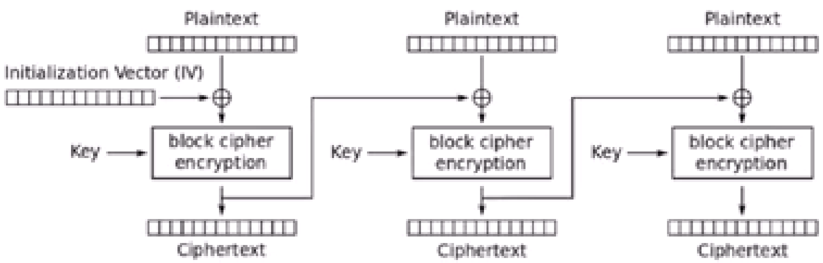
To fix the "same block problem", cryptographers invented different block modes:

Electronic Code Book (ECB)

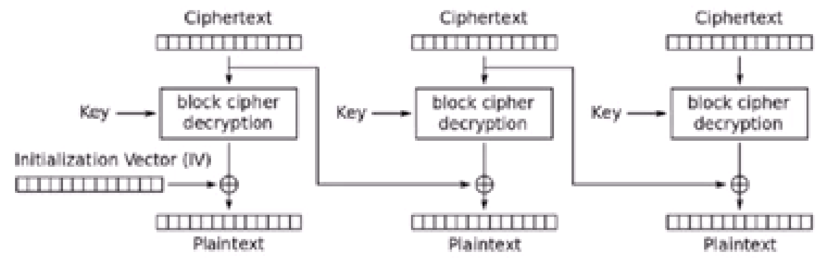
- Encrypts each block individually; bad idea!

Cipher Block Chaining (CBC)

- Chains each block; see picture below
- Needs **initialization vector** (random value; is not part of the key → not a secret)



CBC Encryption

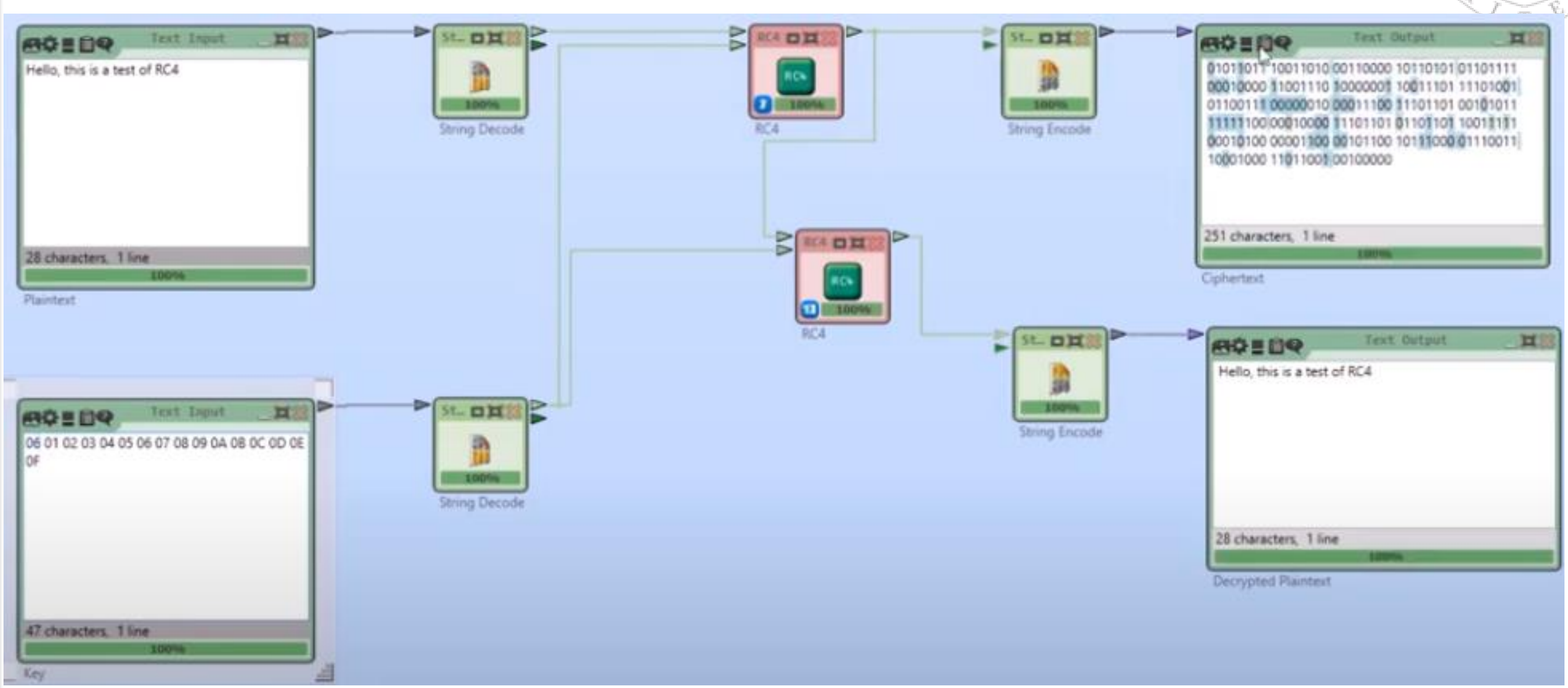


CBC Decryption

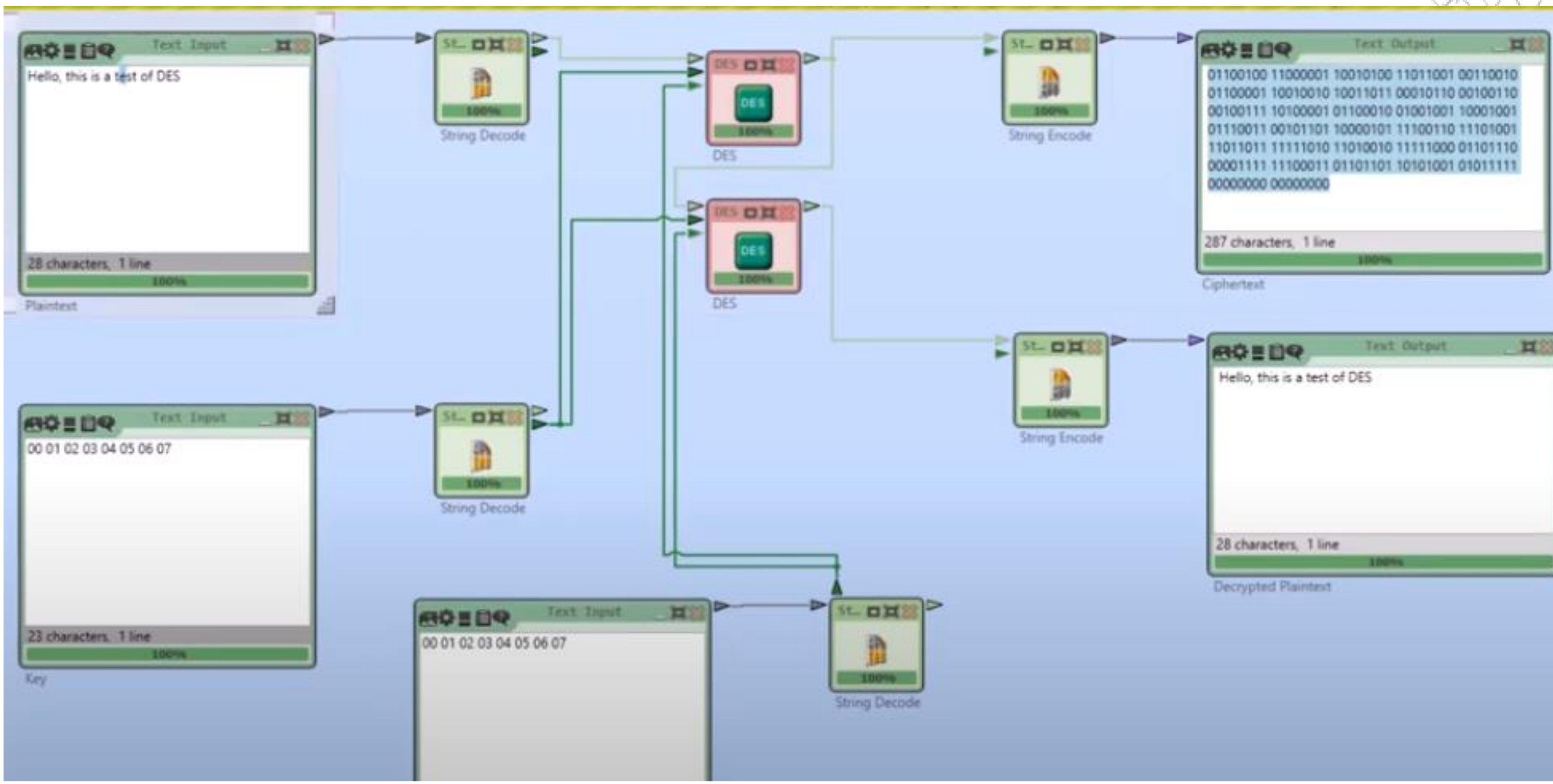
Modern Cryptography

- **Task 1:** **Have a look at a modern stream cipher in CrypTool 2**
- **Task 2:** **Have a look at a modern block cipher in CrypTool 2**
- **Task 3:** **Have a look at block modes in CrypTool 2**

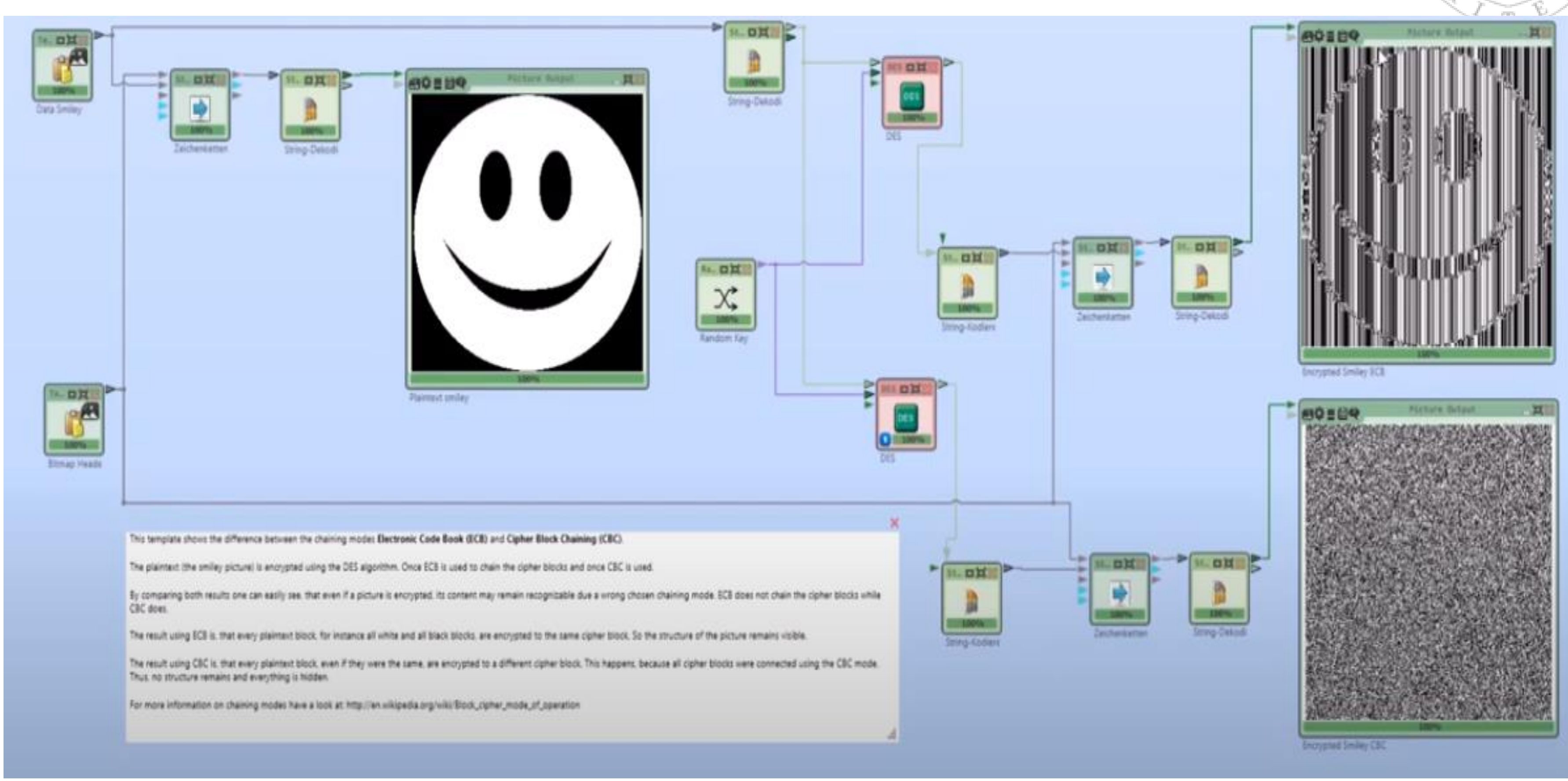
Modern Cryptography



Modern Cryptography



Modern Cryptography



Cryptology for IoT

Modules M4, M6, M8
Session of 26th May, 2022.

M8.1 Briefing of the session
M8.2 Modern Cryptography
M8.3 Modern Cryptanalysis

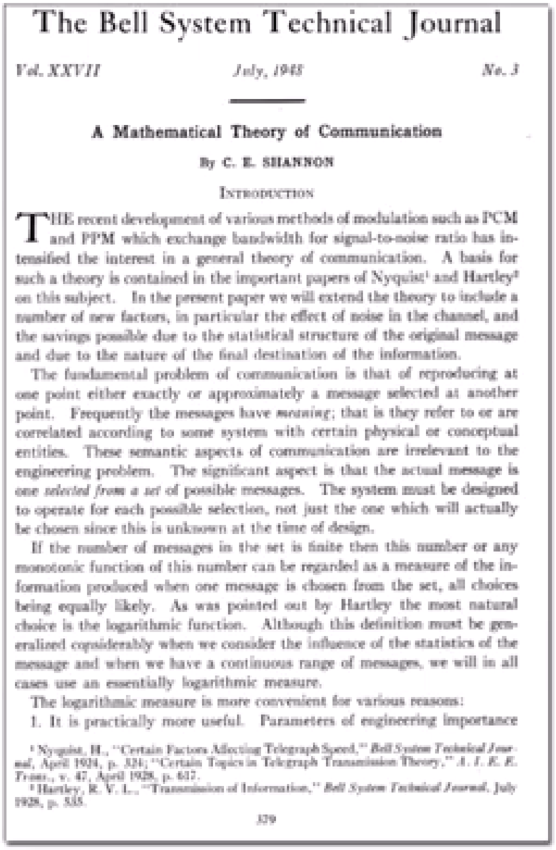
Prof.: Guillermo Botella

Modern Cryptanalysis

Entropy & Shannon's Entropy

Entropy and Brute-Force Attack

Modern Asymmetric Ciphers



The Bell System Technical Journal

Vol. XXVII July, 1948 No. 3

A Mathematical Theory of Communication

By C. E. SHANNON

INTRODUCTION

THE recent development of various methods of modulation such as PCM and PPM which exchange bandwidth for signal-to-noise ratio has intensified the interest in a general theory of communication. A basis for such a theory is contained in the important papers of Nyquist[1] and Hartley[2] on this subject. In the present paper we will extend the theory to include a number of new factors, in particular the effect of noise in the channel, and the savings possible due to the statistical structure of the original message and due to the nature of the final destination of the information.

The fundamental problem of communication is that of reproducing at one point either exactly or approximately a message selected at another point. Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem. The significant aspect is that the actual message is one *selected from a set* of possible messages. The system must be designed to operate for each possible selection, not just the one which will actually be chosen since this is unknown at the time of design.

If the number of messages in the set is finite then this number or any monotonic function of this number can be regarded as a measure of the information produced when one message is chosen from the set, all choices being equally likely. As was pointed out by Hartley the most natural choice is the logarithmic function. Although this definition must be generalized considerably when we consider the influence of the statistics of the message and when we have a continuous range of messages, we will in all cases use an essentially logarithmic measure.

The logarithmic measure is more convenient for various reasons:

1. It is practically more useful. Parameters of engineering importance

[1] Nyquist, H., "Certain Factors Affecting Telegraph Speed," *Bell System Technical Journal*, April 1924, p. 324; "Certain Topics in Telegraph Transmission Theory," *A. I. E. E. Trans.*, v. 47, April 1928, p. 617.
[2] Hartley, R. V. L., "Transmission of Information," *Bell System Technical Journal*, July 1928, p. 535.

379

Shannon, Claude E.: "A Mathematical Theory of Communication." Bell system technical journal 27.3 (1948): 379-423

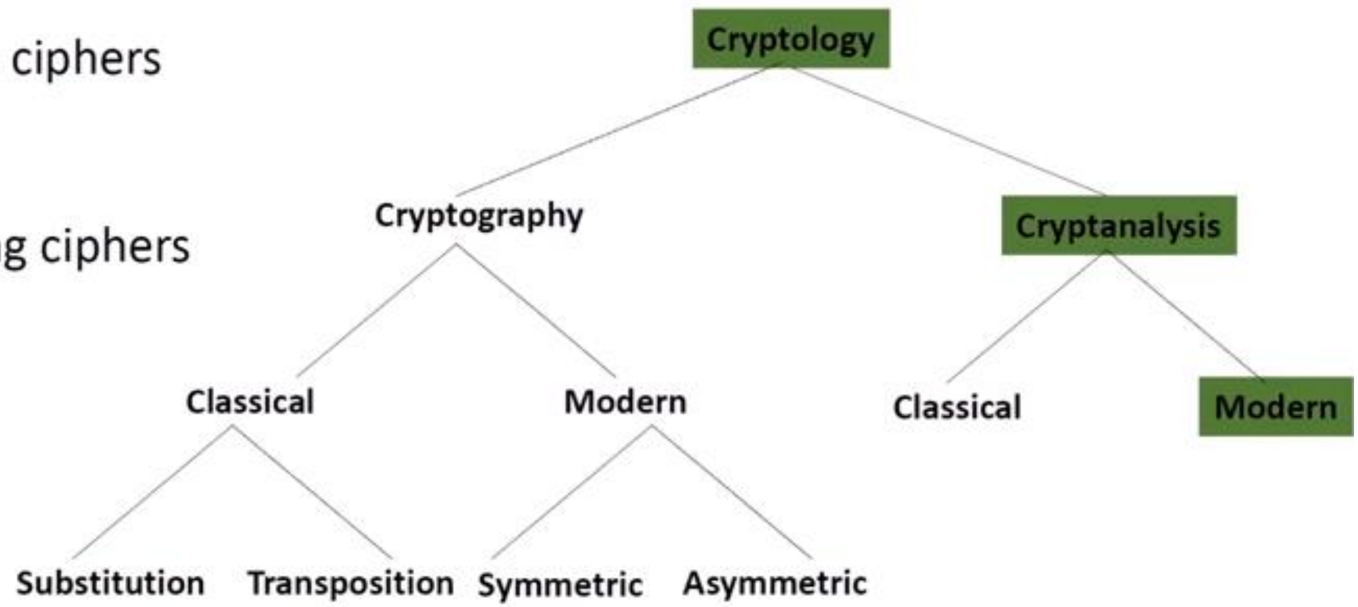
Modern Cryptanalysis

Cryptography

Art of making ciphers

Cryptanalysis

Art of breaking ciphers



Modern Cryptanalysis

- Basic idea of entropy comes from the physics of the 19th century
- Measure of disorder of a physical system
- “The entropy of an isolated system never decreases over time” (2nd law of thermodynamics)
- Boltzmann extended the idea 1877 further to an information theoretical approach. Systems go from a less likely to a more likely state. This increases the value of the entropy
- Claude E. Shannon (next slide) used the term „entropy“ in 1948 for the loss of information in data communication. He obtained the idea to call it entropy by John von Neumann

Modern Cryptanalysis

- Entropy H (aka as information entropy)
- Invented by Claude E. Shannon in 1948 and published in "A Mathematical Theory of Communication" (see first slide)
- Measure for the uncertainty of a random variable
  - Measure of disorder, unpredictability
  - Quantifies the expected value of information
  - Absolute limit for the best possible lossless compression
- Examples
  - Single toss of a fair coin: Entropy $H = 1$ bit
  - Single toss of a coin with two heads/tails: Entropy $H = 0$
  - Single toss of an unfair coin: $0 \leq H \leq 1$

Module 8: Cryptology for IoT

Modern Cryptanalysis

- Entropy $H(X)$ of a discrete random variable X with possible values $\{x_1, x_2, \ldots, x_n\}$
- Probability of each x_i is $p(x_i)$. Each $p(x_i)$ value is between 0 and 1 (sum of all $p(x_i)$ is 1)
- Information content/uncertainty of X is $I(X)$
  - $H(X)$ is the expected value E of $I(X)$, thus, $H(X) = E(I(X))$
  - $I(x_i) \;= \log_b \frac{1}{p(x_i)} = -\log_b(p(x_i)), \forall i \in \{1,2,\ldots,n\}$
  - $H(X) = \sum_{i=1}^{n} p(x_i) I(x_i) = \sum_{i=1}^{n} p(x_i) \log_b \frac{1}{p(x_i)} = -\sum_{i=1}^{n} p(x_i) \log_b p(x_i)$
- Unit of the entropy
  - b = 2 → bit
  - b = e → nat
  - b =10 → dit

Modern Cryptanalysis

- Example of entropy calculation
- We have 26 different letters in English using a Latin alphabet A,B,C,…,Z
- Example text is “HELLOWORLD”

1. Count each letter: H = 1, E = 1, L = 3, O = 2, W=1, R=1, D=1
2. Calculate frequencies of letters: $p_H=\frac{1}{26}$, $p_E=\frac{1}{26}$, $p_L=\frac{3}{26}$, $p_O=\frac{2}{26}$, $p_W=\frac{1}{26}$, $p_R=\frac{1}{26}$, $p_D=\frac{1}{26}$
3. Compute entropy value:

$$H = -(\left(\frac{1}{26}\right)\log_2\left(\frac{1}{26}\right) + \left(\frac{1}{26}\right)\log_2\left(\frac{1}{26}\right) + \cdots + \left(\frac{1}{26}\right)\log_2\left(\frac{1}{26}\right)) \approx 1{,}548 \text{ bit}$$

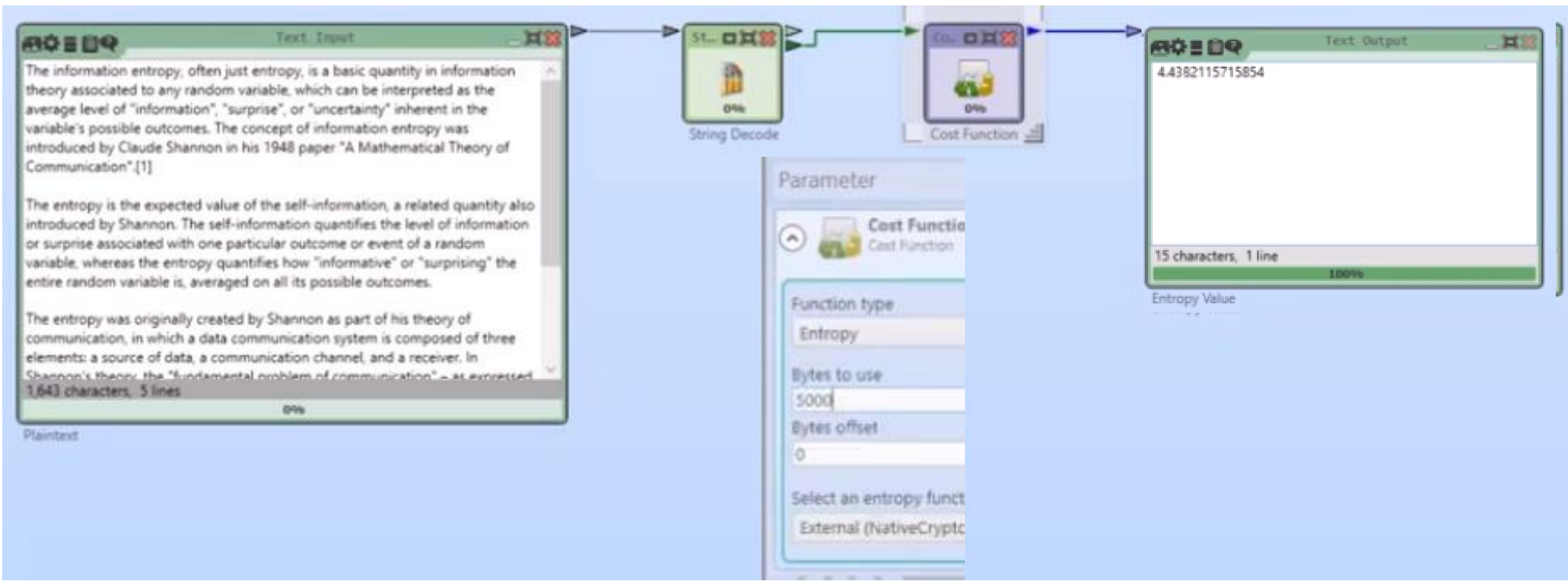
Modern Cryptanalysis

- In cryptanalysis, we can use the entropy as a "cost function" to rate a text
- **Plaintext**
  - Natural language
  - Low disorder: low "information content" → low entropy
- **Ciphertext**
  - Encrypted; randomized characters (or with modern ciphers randomized bits)
  - High disorder (chaos): high "information content" → high entropy
- Useful for brute-force attacks (aka exhaustive key searching attacks)
  1. Decrypt ciphertext using every possible key
  2. Calculate for each putative plaintext its entropy value
  3. Keep putative plaintexts with lowest entropy (e.g. 100 "best" plaintexts)
  - With very high probability, the original plaintext is in this set
  - English text (only 26 different letters) has an entropy value between 0.6 bit and 1.3 bit per character
  - Having an English text but using a byte for representing a single character, since we have 256 different possibilities, English text then has an average entropy value of around 4.7 bit

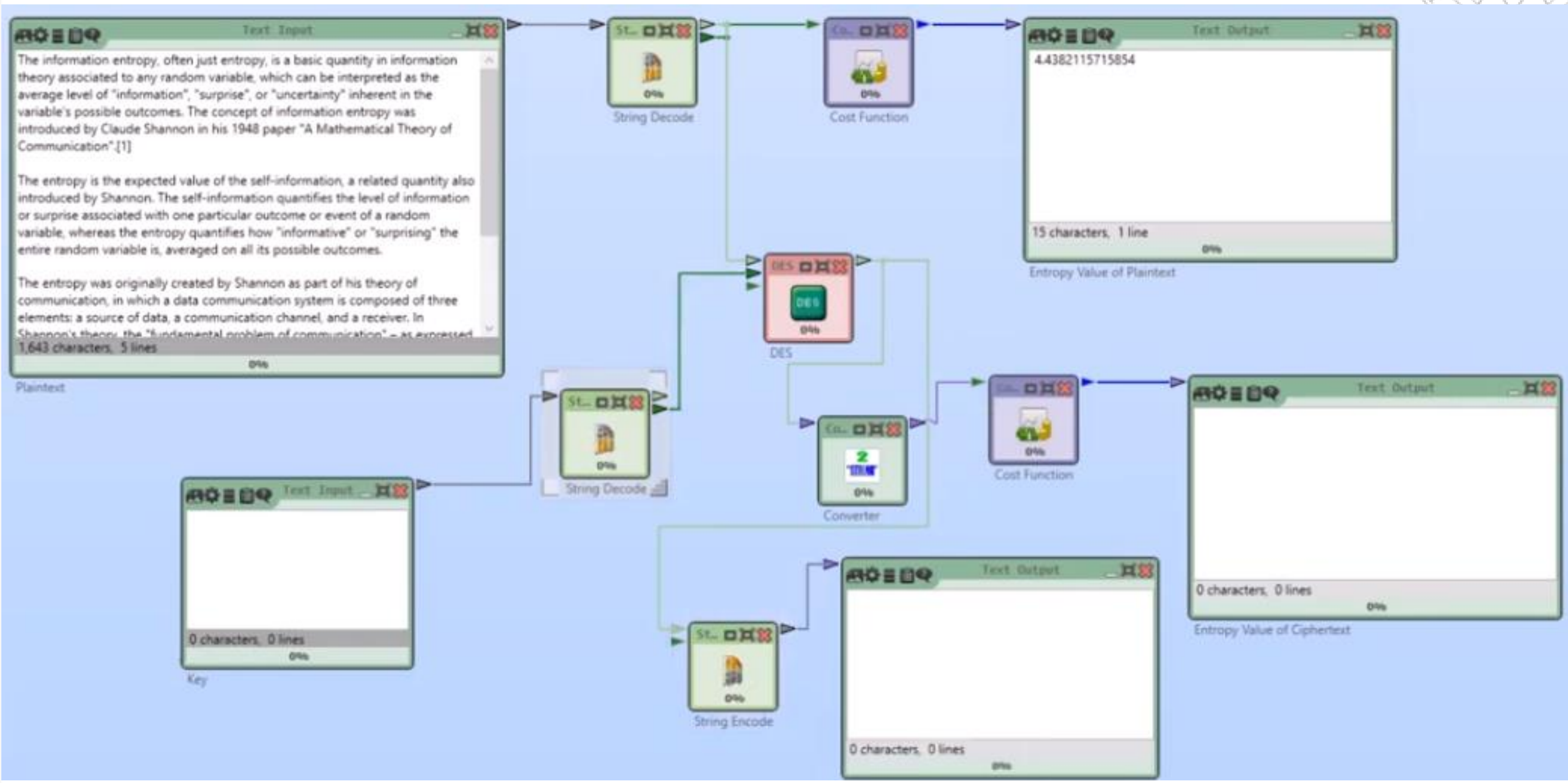
Modern Cryptanalysis

- **Task 1:** Have a look at the CT2 Cost Function component (besides other statistics, it also offers entropy as cost function)
- **Task 2:** Encrypt a text using the DES cipher
- **Task 3:** Break the DES encrypted ciphertext with reduced keyspace using the KeySearcher component of CT2

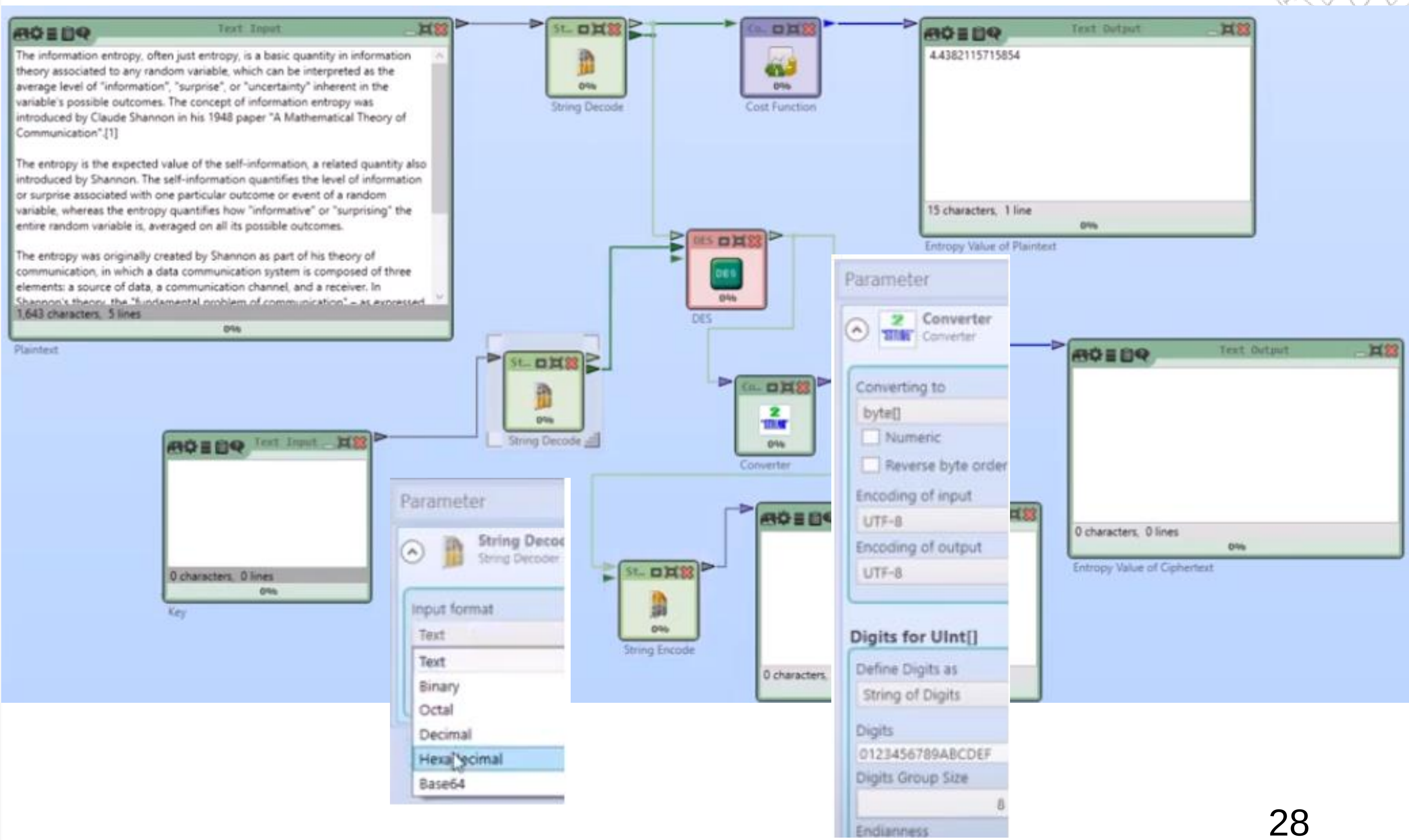
Modern Cryptanalysis



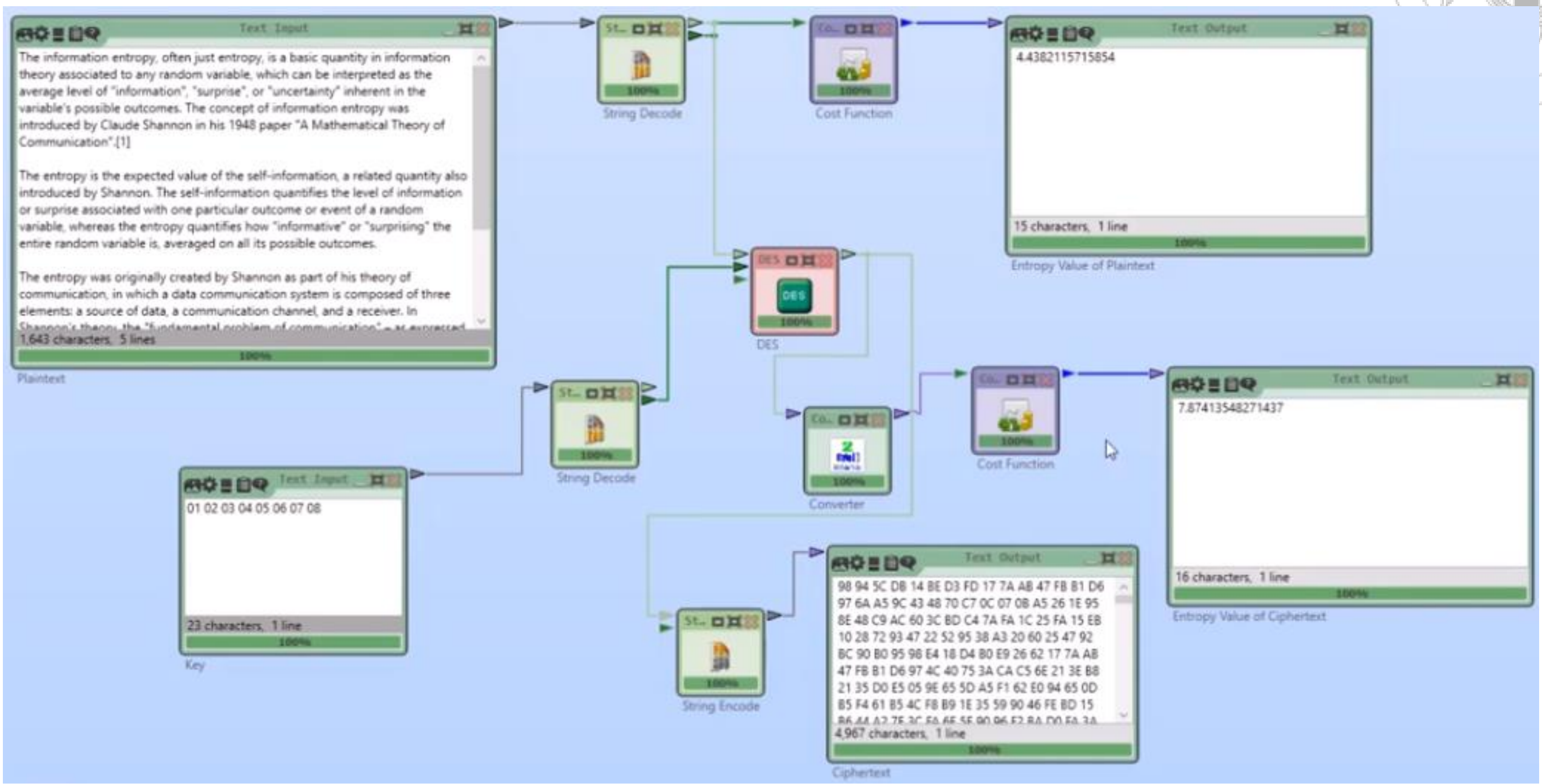
Modern Cryptanalysis



Modern Cryptanalysis

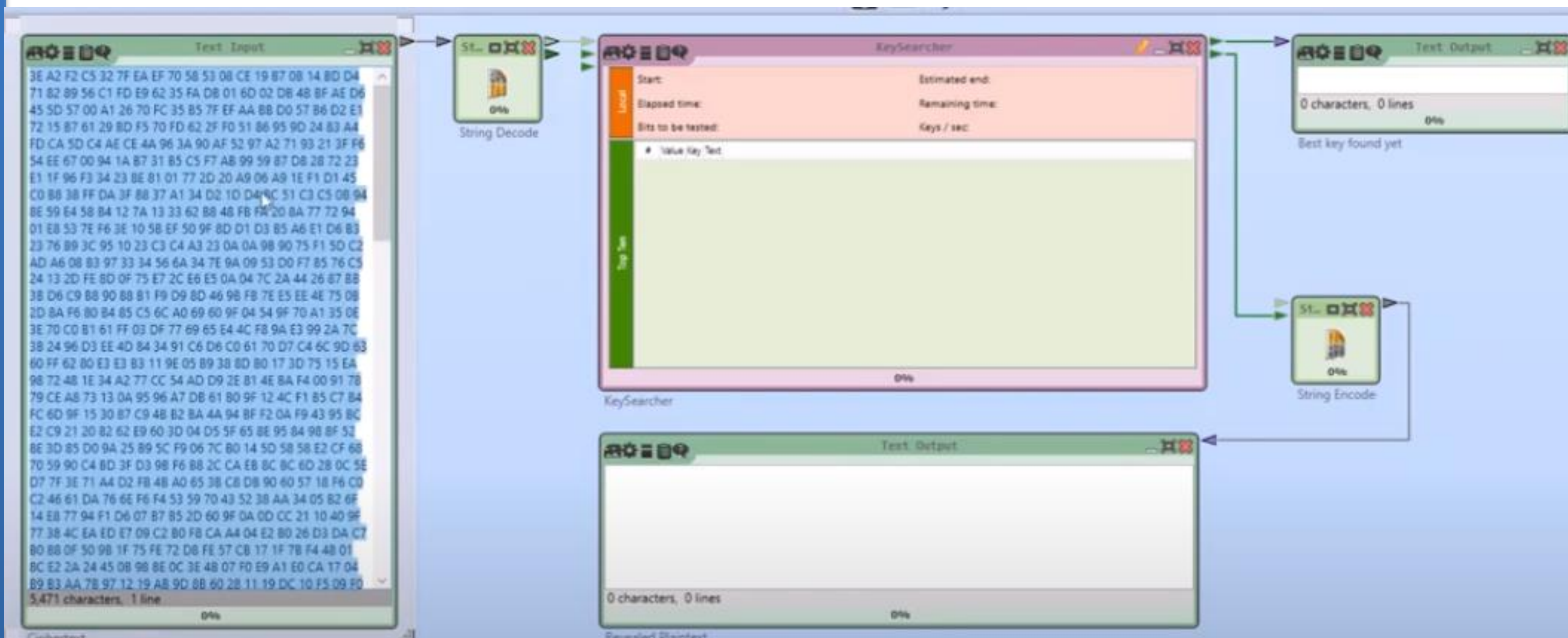


Modern Cryptanalysis



– Entropy of the ciphertext grows up (4.4 to 7.8)

Modern Cryptanalysis



– Using template DES analysis entropy

Modern Cryptanalysis

– Using template DES analysis entropy

Modern Cryptanalysis

– Using template DES analysis entropy

Cryptology for IoT

Modules M4, M6, M8
Session of 26th May, 2022.

M8.1 Briefing of the session
M8.2 Modern Cryptography
M8.3 Modern Cryptanalysis

Prof.: Guillermo Botella