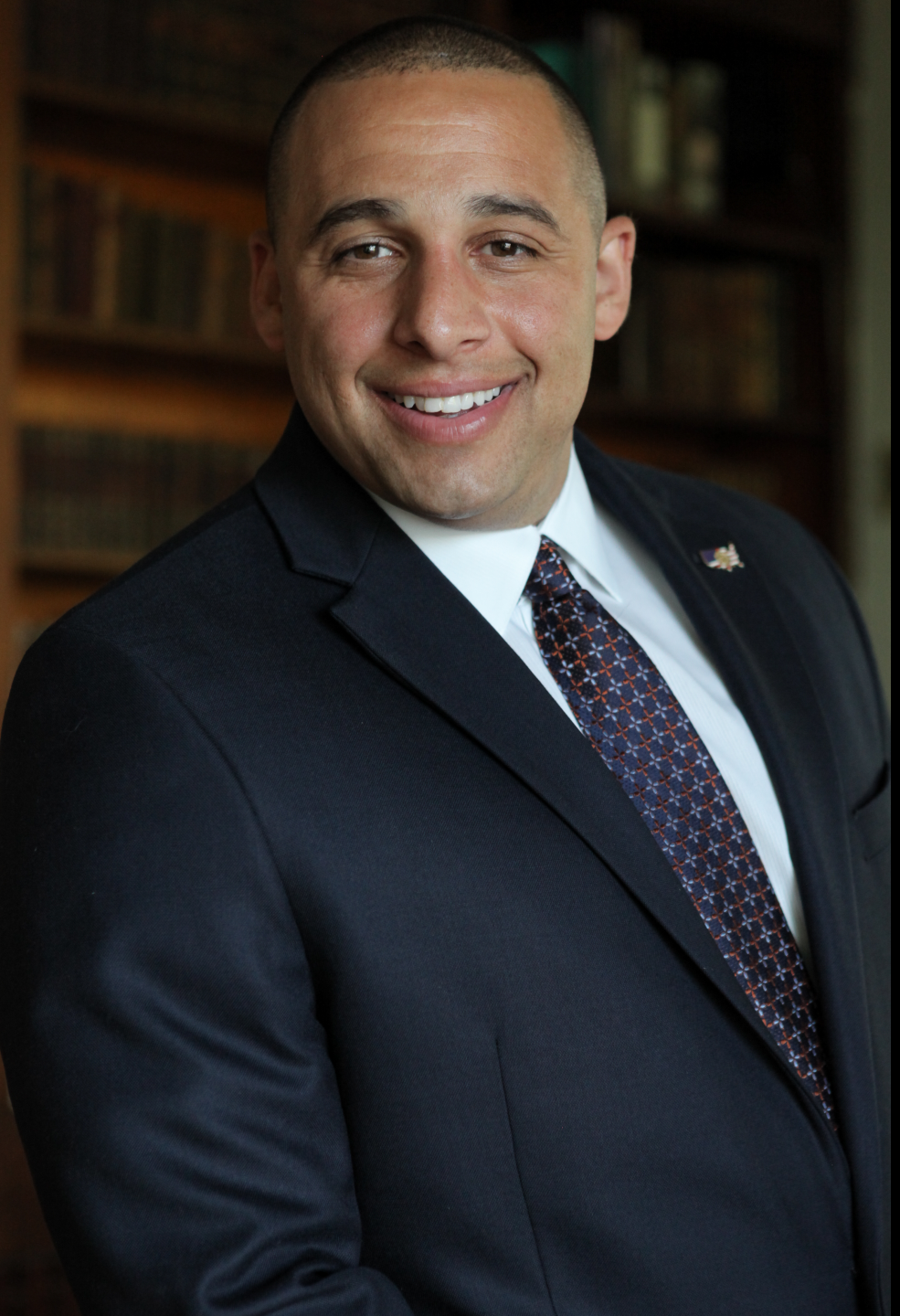
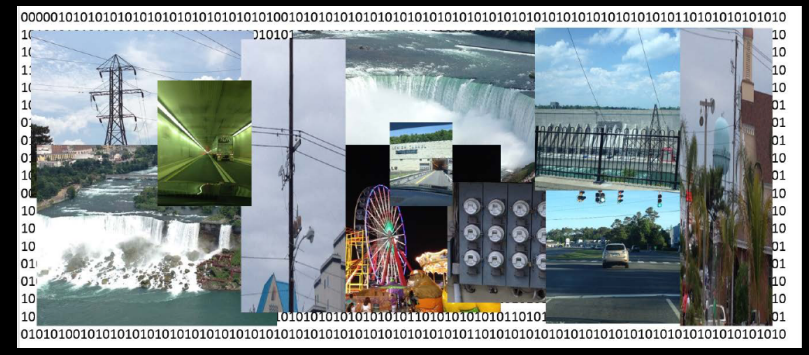


Advanced Symmetric Cryptography Concepts



Dr. Dwayne Hodges, USA, (Ret.)

CISSP, CCISO, CEH, CNDA, ECES, SEC+ ITIL

Advanced Symmetric Cryptography Concepts

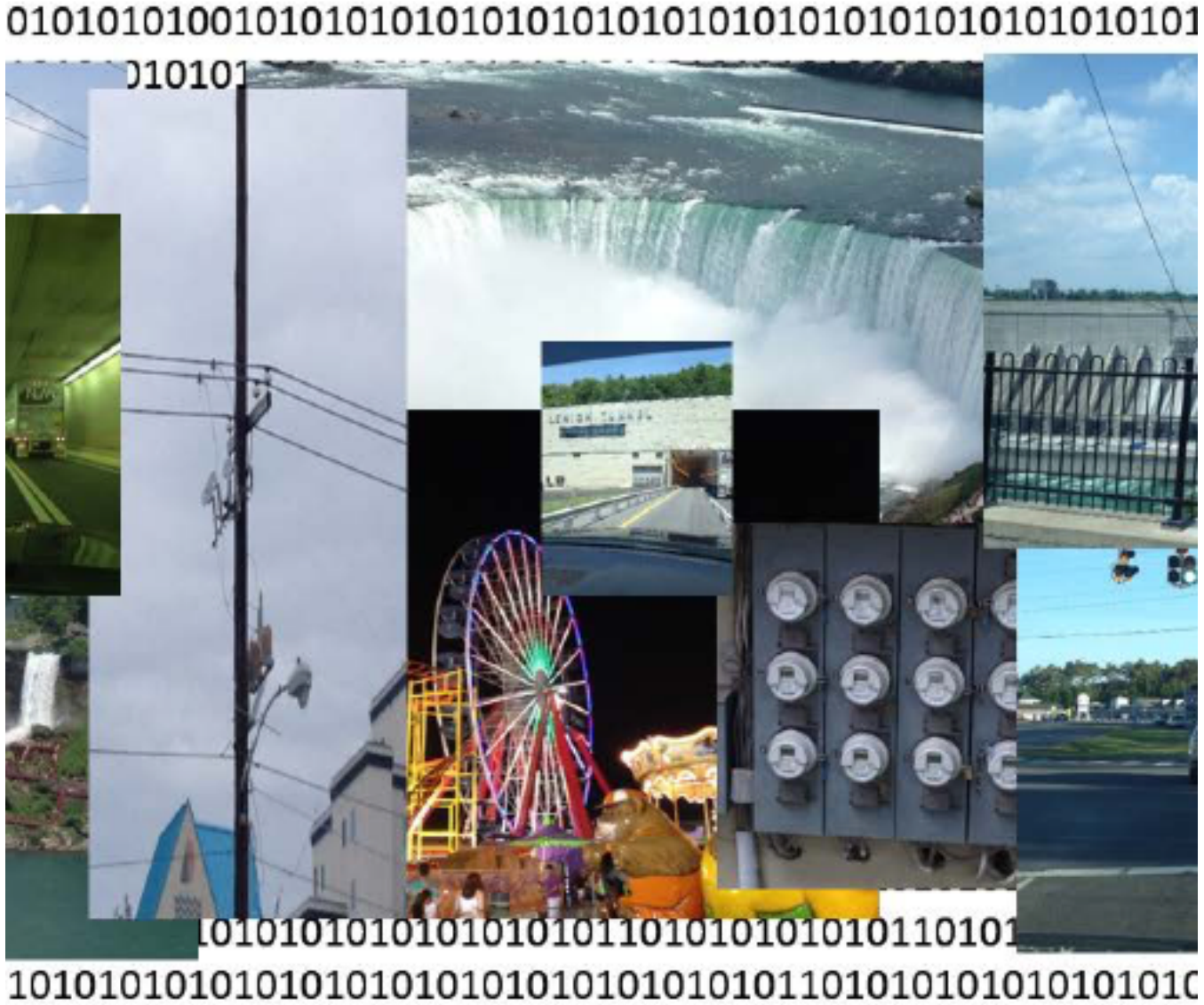
- Goals of Cryptography
  - Confidentiality
  - Integrity
  - Availability
  - Non-Repudiation

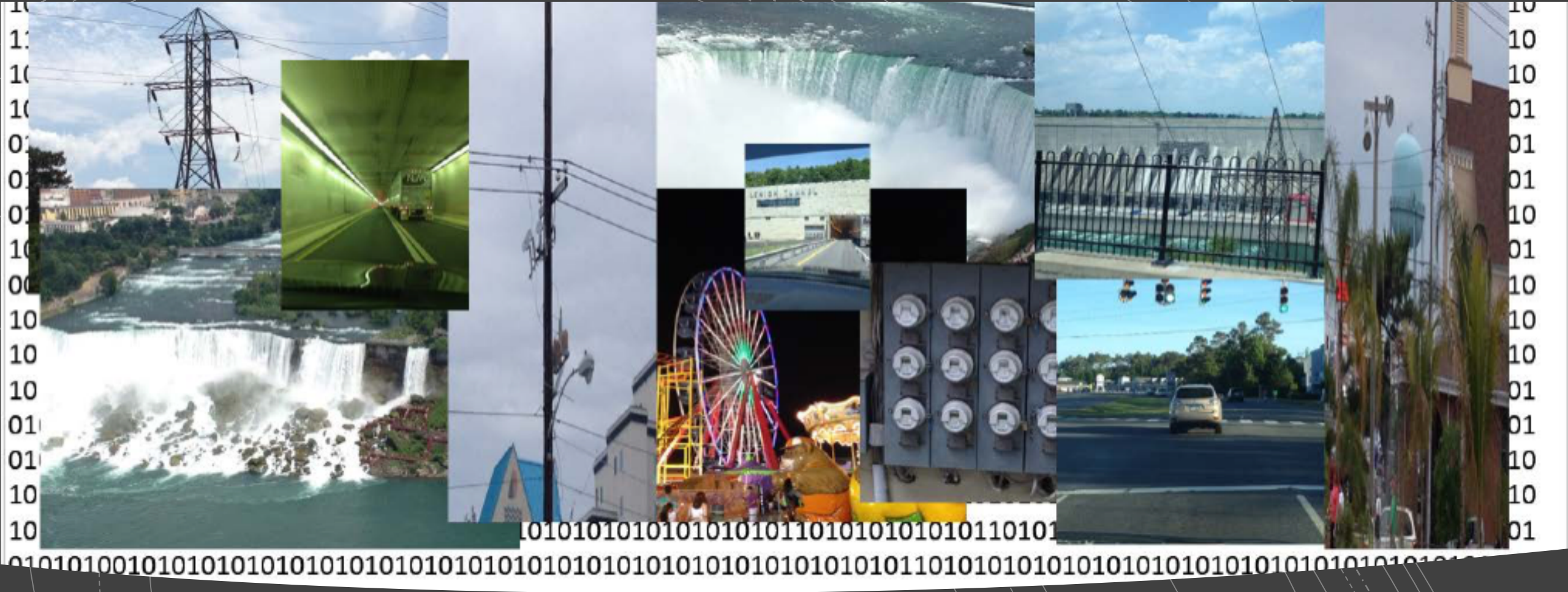
Advanced Symmetric Cryptography Concepts

- **Substitution**
- **Transposition**

Advanced Symmetric Cryptography Concepts

- Confusion is the attempt to remove the letter frequency characteristics in the plain text from appearing in the cypher text.
  - This is done using ***substitution*** operations
- Diffusion is where a change to one character in the plain text affects multiple characters in the cipher test.
  - This is done using ***transposition*** operations
- when done correctly, confusion and diffusion create an **Avalanche effect**
  - **Meaning -** small changes in the plaintext results in large effects in the output cyphertext





Advanced Symmetric Cryptography Concepts

- Stream ciphers- bit by bit
- Block ciphers- collection of bit

Advanced Symmetric Cryptography Concepts

Cryptography: the science of transforming information into an unintelligible form

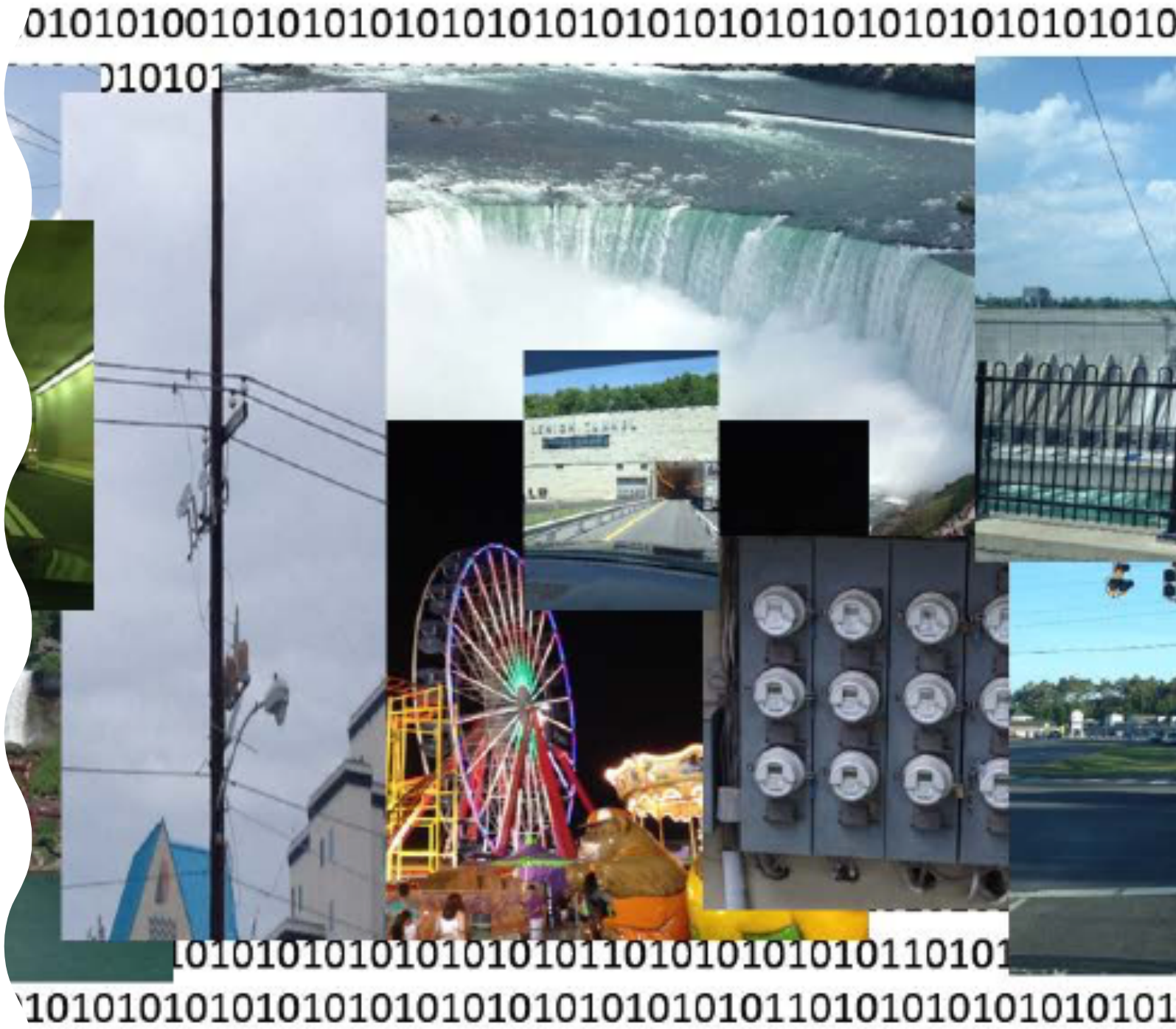
Cryptanalysis: the study and practice of finding weaknesses in ciphers

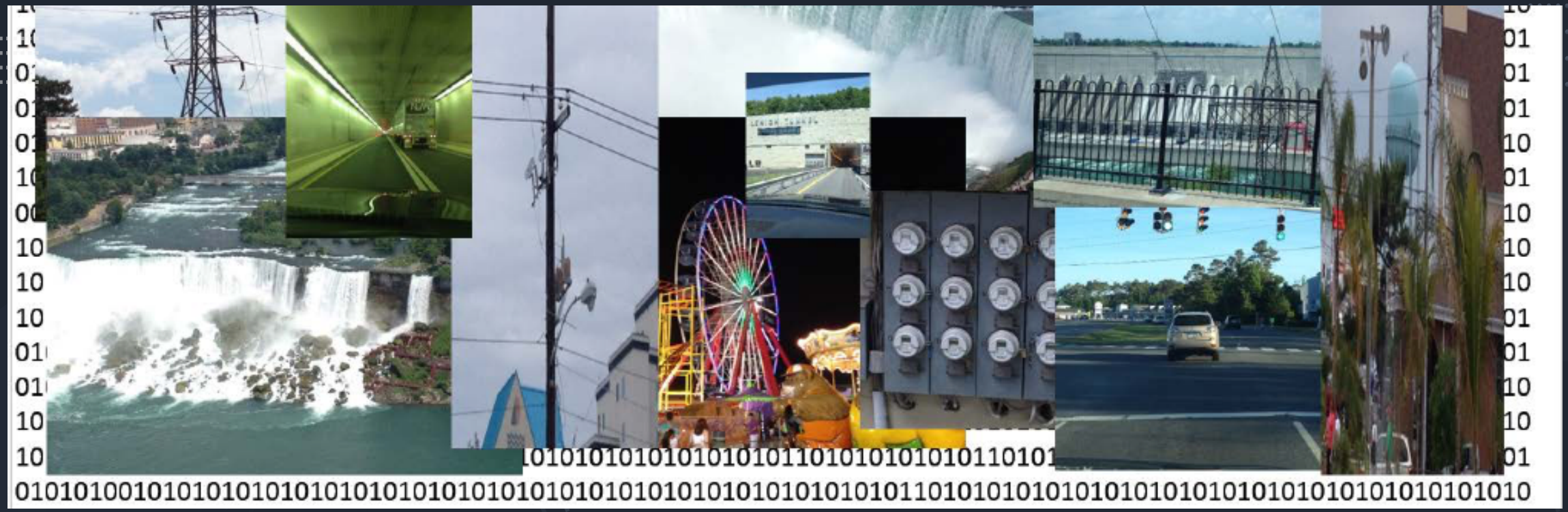
Algorithm: the series of steps/processes/formulas that are followed to arrive at a result

Cipher: a method used to encode characters to hide their value

Decipher- the process of decrypting encrypted text

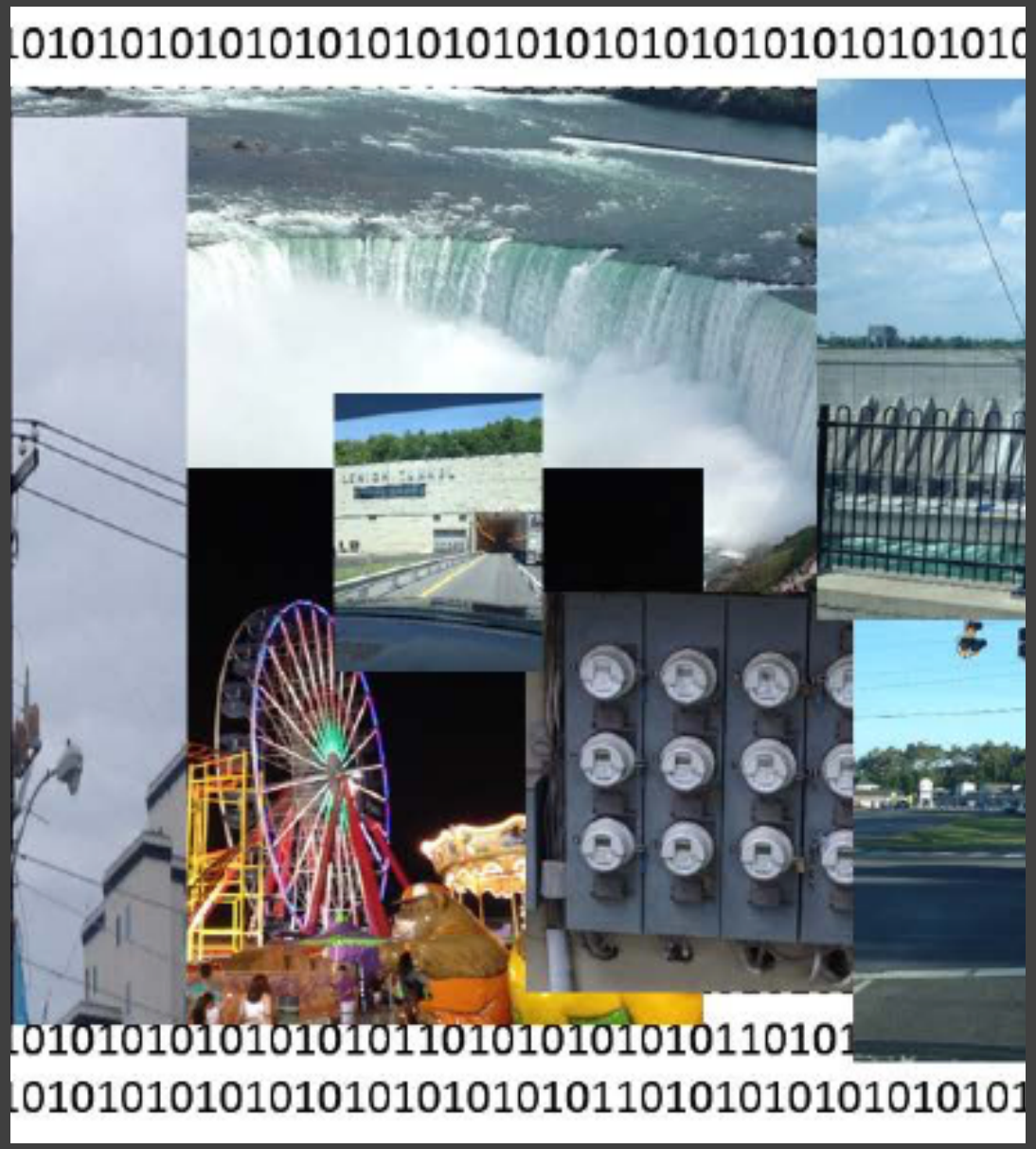
Plain text: information which is transferred or stored without cryptographic protection





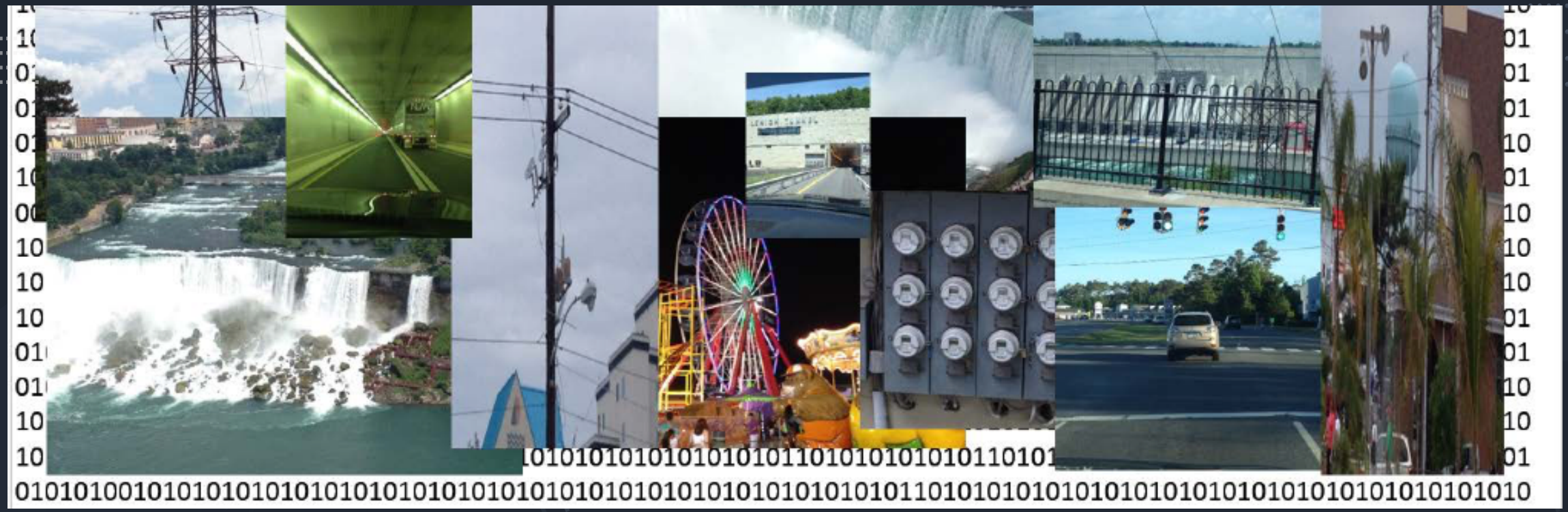
Advanced Symmetric Cryptography Concepts

- **Cryptology**-the study of both cryptography and cryptanalysis
- **Cryptosystem**- all the part or pieces that make up a system to carry out the encryption and decryption process
- **Key Clustering-** instance when to different keys generate the same cipher text



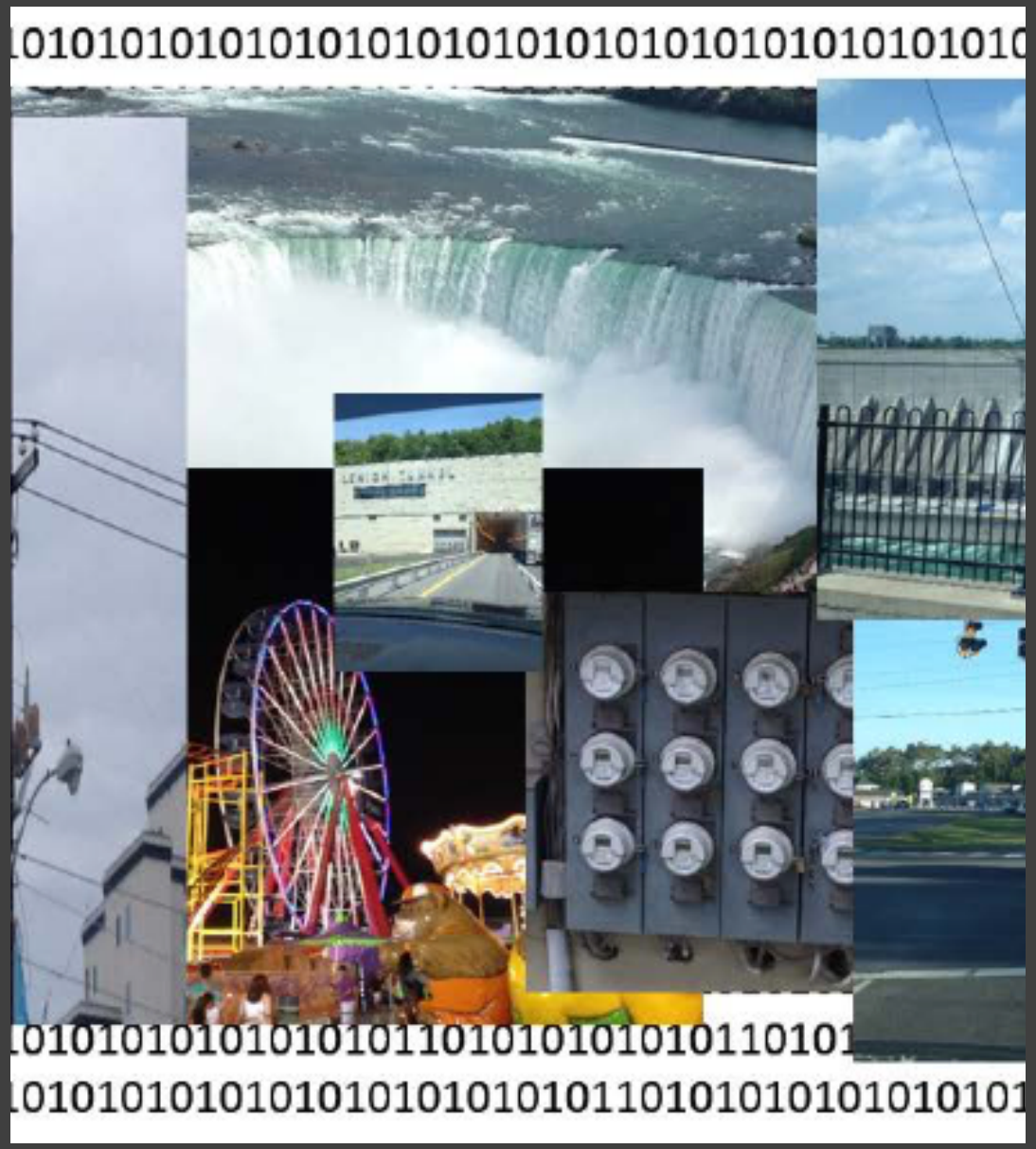
Advanced Symmetric Cryptography Concepts

- Typically, the Algorithm not the secret piece, the secret values(key) are
- Key is a large set of random numbers
- Primitive- Mathematical function within an algorithm
- Key works by telling the how to work, and this is encryption works ,
  - by changing the plane text (readable) in cipher text (unreadable)
- Key space is a large set of values the algorithm and the key generation occurs by choose key from the key space
  - The large the value, the more space, the stronger the algorithm, the more secure



Advanced Symmetric Cryptography Concepts

- a.k.a. Secret Key, Shared Key, Same Key, Single Key, Session Key
- Best suited for bulk encryption; much faster than asymmetric cryptography
- Both parties share the same key



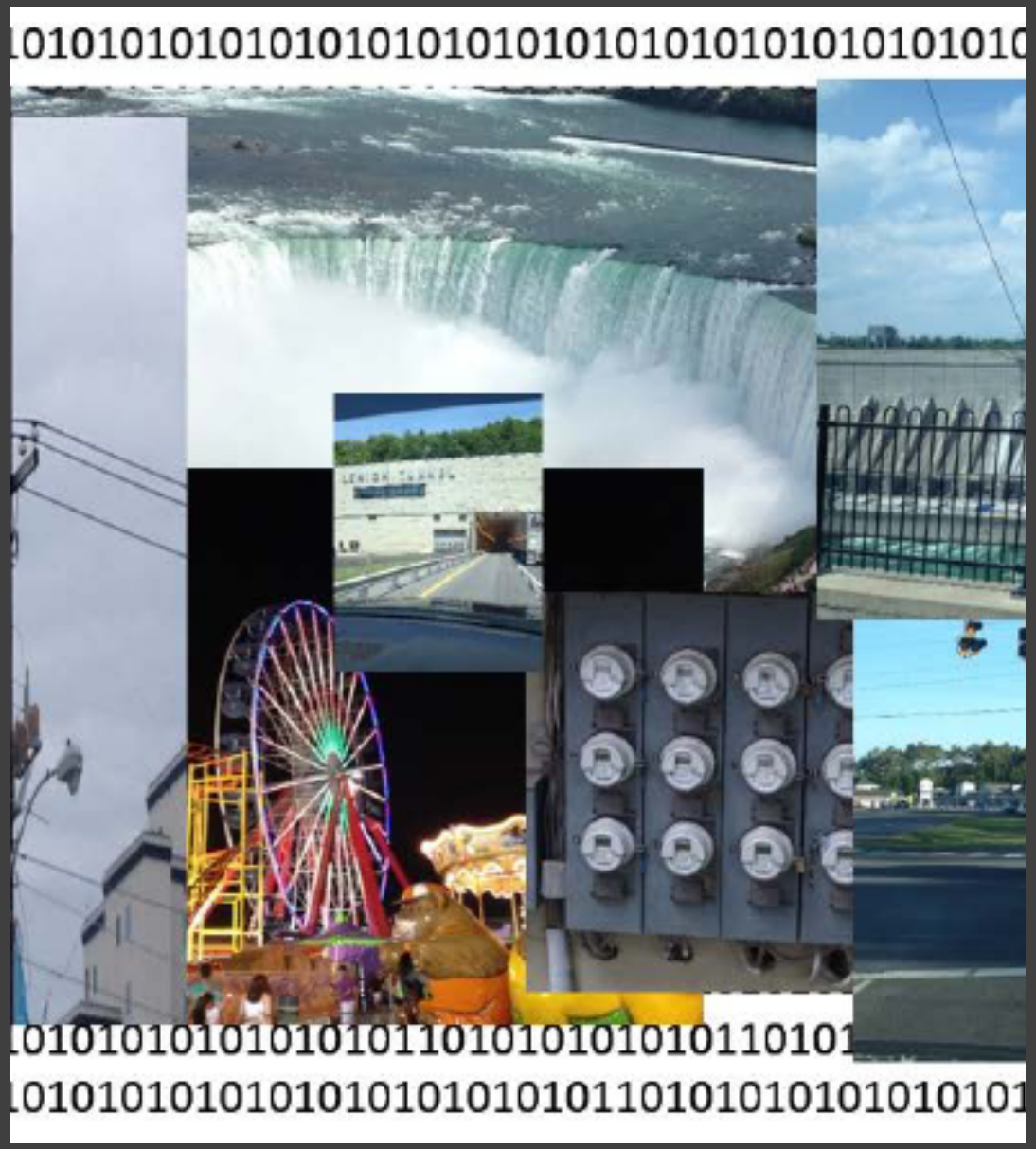
Advanced Symmetric Cryptography Concepts

- Advantages:
  - Less computationally intensive
  - Produces a smaller file size
  - Allows for faster transmissions
- Disadvantages
  - Exchanging of the shared secret key
  - Trust between parties sharing the key
  - Management of keys: $n(n - 1)/2$
  - No authentication or non-repudiation

Advanced Symmetric Cryptography Concepts

Binary Code, XOR, OR, AND

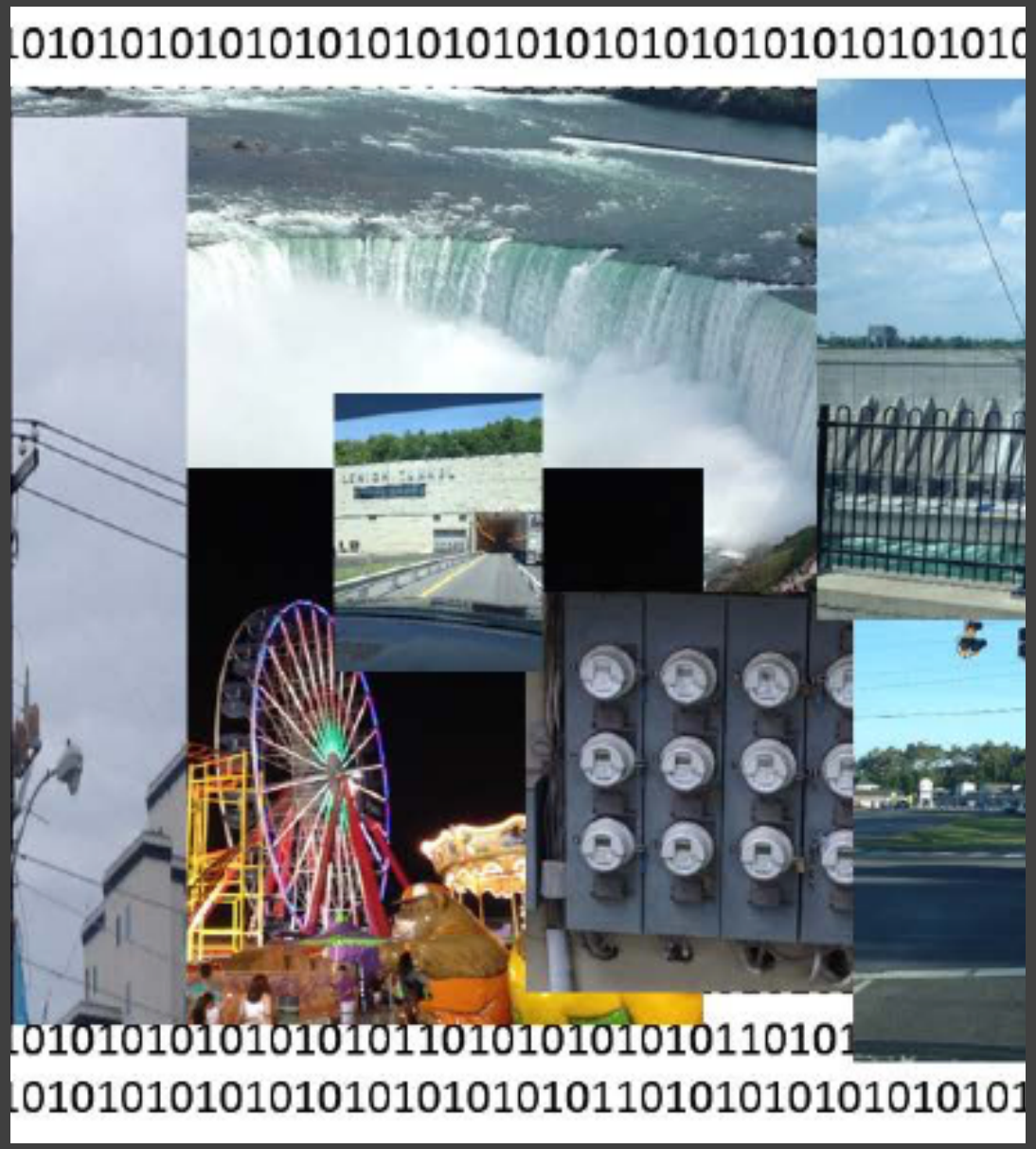
- Arguments, combines 1s, and 0s
- Exclusive OR Binary function- “ combine “0s” and “1”s
- if two bits are the same, the result is 0, if they are different the result is 1



Advanced Symmetric Cryptography Concepts

- **Binary XOR**
- Possible because of binary code
- XOR compares each of the “1”s and “0”s in sequence
- If they are the same, the result is “0”
- If they are different the result is “1”
- Mathematical operation, this is how basic encryption starts, not hard or **true**

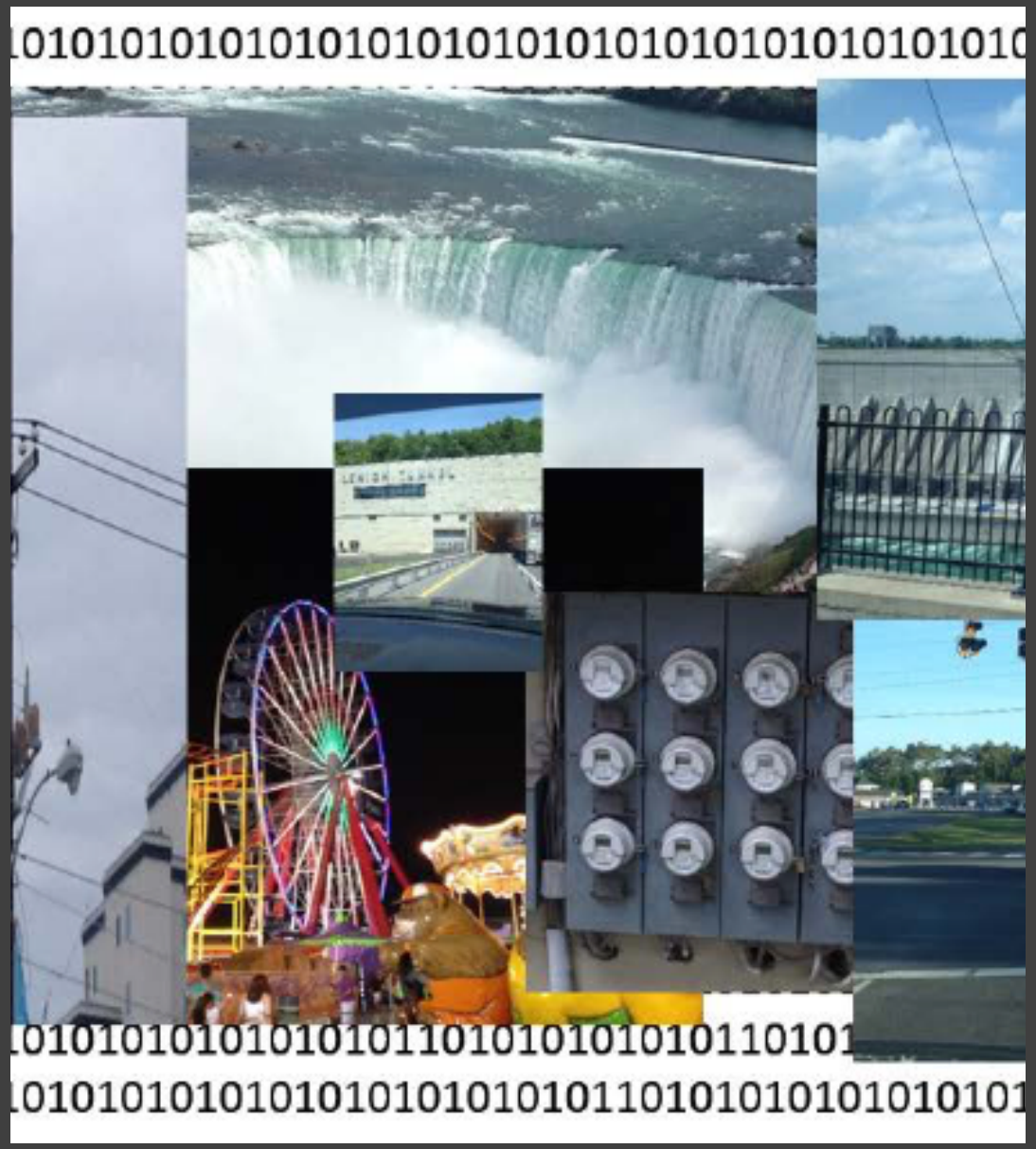
- 101001
- 001011
- 100010



Advanced Symmetric Cryptography Concepts

- **Binary AND**
- The **binary** AND operation (also known as the **binary** AND **function**) " **if A is true and B is true (A AND B), it is True-**
- will always produce a 1 output if both of its inputs are 1 and
- will produce a 0 output if one or both of its inputs are 0.

- 101101
- 011011
- 001001



Advanced Symmetric Cryptography Concepts

- **Binary OR**
- “Logical functions”
- It is like the ADD operation which takes two arguments (two inputs) and produces one result (one **output**).
- The binary OR operation (also known as the binary OR function) will always produce a 1 **output** if either of its inputs are 1 and will produce a 0 **output** if both of its inputs are 0.
- ***“If A is TRUE or B is TRUE then (A OR B) is TRUE”***
- 101001
- 001011
- 101011

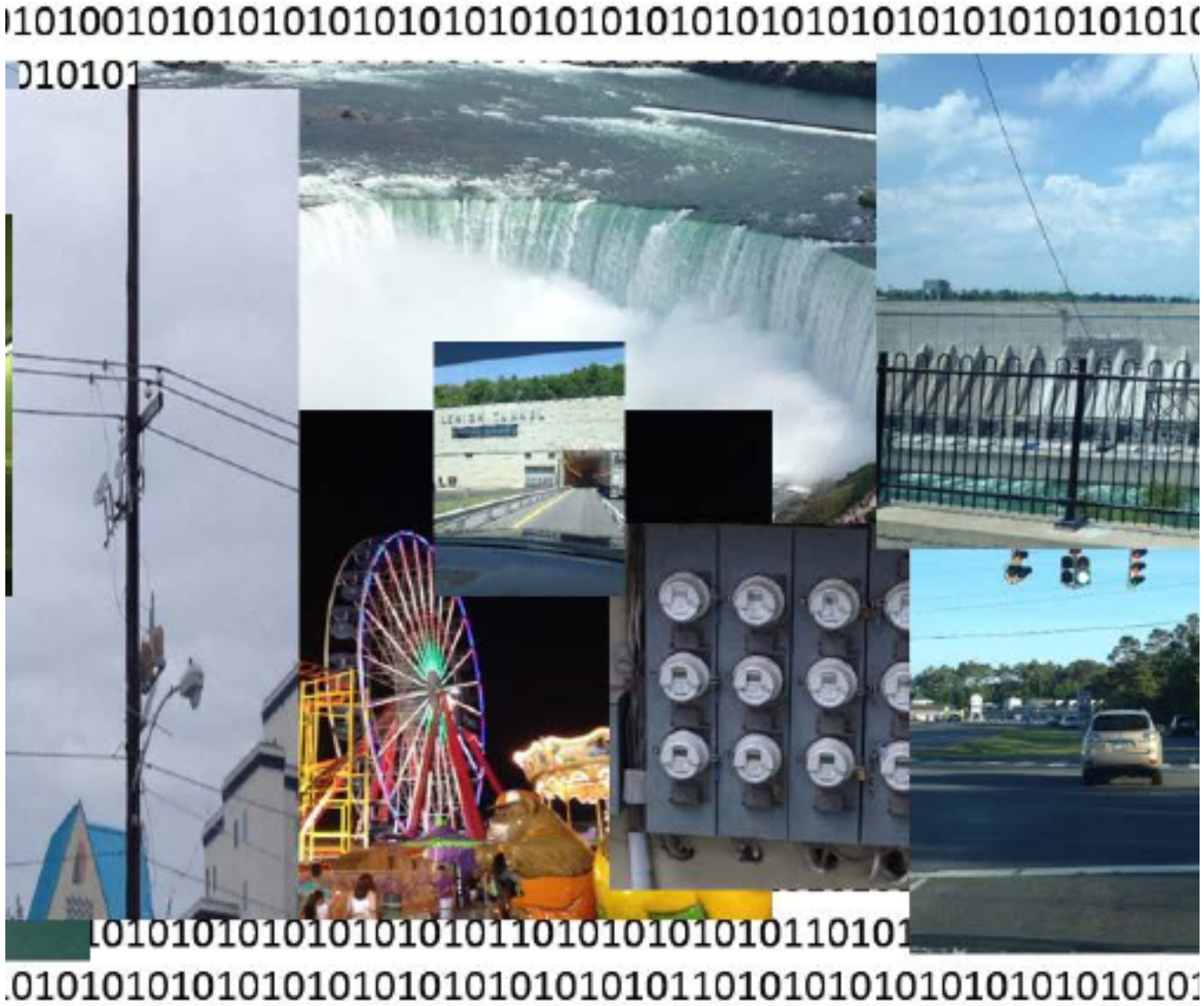
Advanced Symmetric Cryptography Concepts

Keys

- **The key is the most important thing, it tells the algorithm how to work**
- **The larger the key size, the more values for key generation, the strong the the algorithm, the hard the work factor**
  - **Entire key space should be used**
  - **Random key generation should be used (IVs)**
  - **Strong keys should be used**
  - **Key should be longer than the message**
  - **Key management and security should be in place**

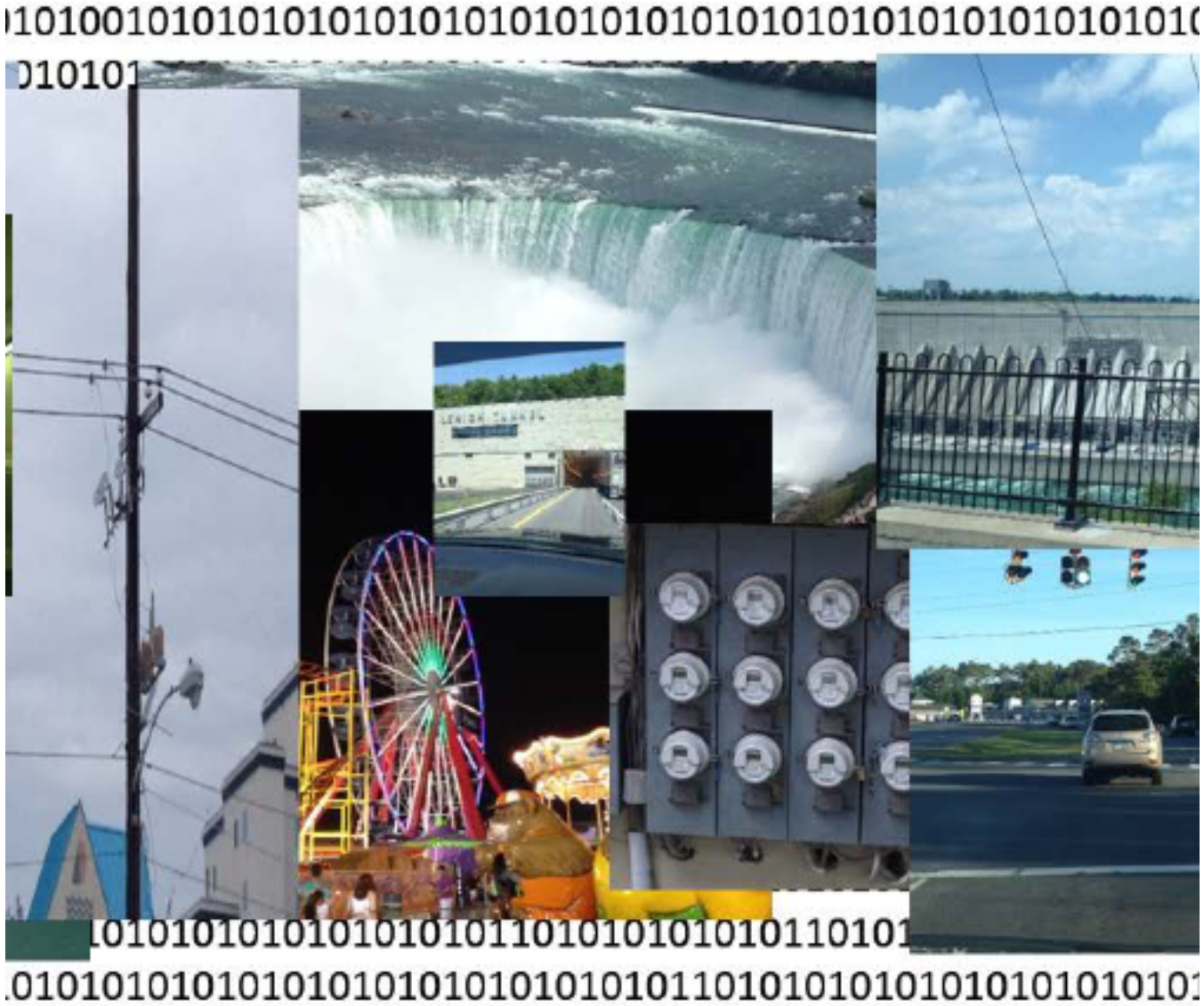
Advanced Symmetric Cryptography Concepts

- DES (Data Encryption Standard) (DEA, Lucifer)
  - Based on IBM's Lucifer algorithm
  - 64-bit block (56-bit key + 8 bits for parity)
  - Algorithm: DEA (Data Encryption Algorithm)
  - Easily broken
- 3DES (Triple-DES)
  - Upgrade of DES (still in use)
  - Applies DES three times
  - 168-bit key (+24 for parity)



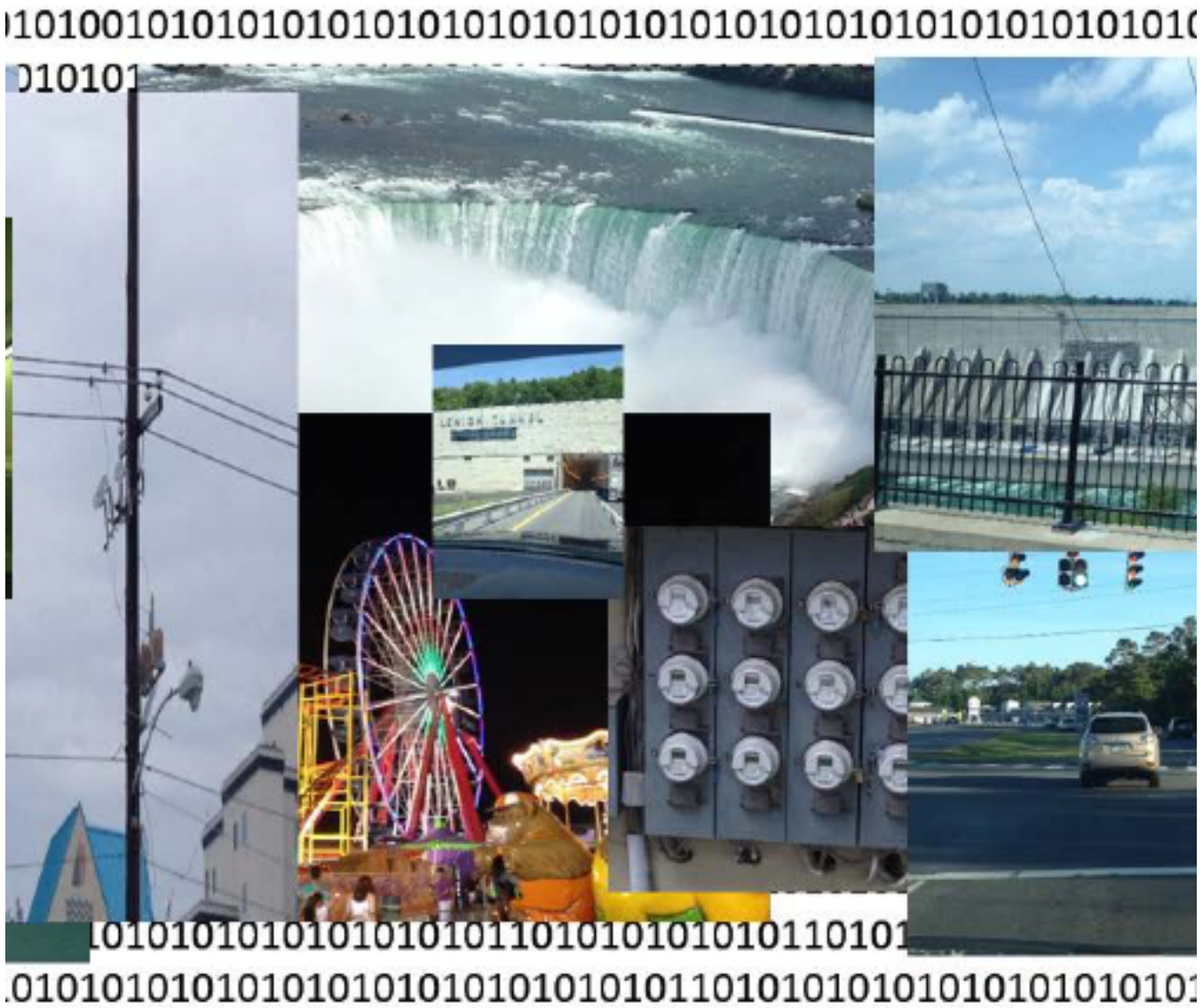
Advanced Symmetric Cryptography Concepts

- IBM
- Developed by Lucifer
- NIST and NSA fought him
- 16 rounds of substitution
- 4 modes
  - ECB (Electric Code Book)
  - CBC (Cipher block chaining)
  - CFB (Cipher feedback Mode)
  - OFB (output feedback mode)
  - CTM (Counter Mode)



Advanced Symmetric Cryptography Concepts

- IV
  - Random values used with algorithms to ensure patterns are not created
  - Used with keys
  - If they are not used, the same plaintext encrypted with same key, will generate same cyphertext
- Error Propagation
  - In some cases, you want to ensure errors do not affect your encryption process, so you use a stream cipher to encrypt small amounts of data

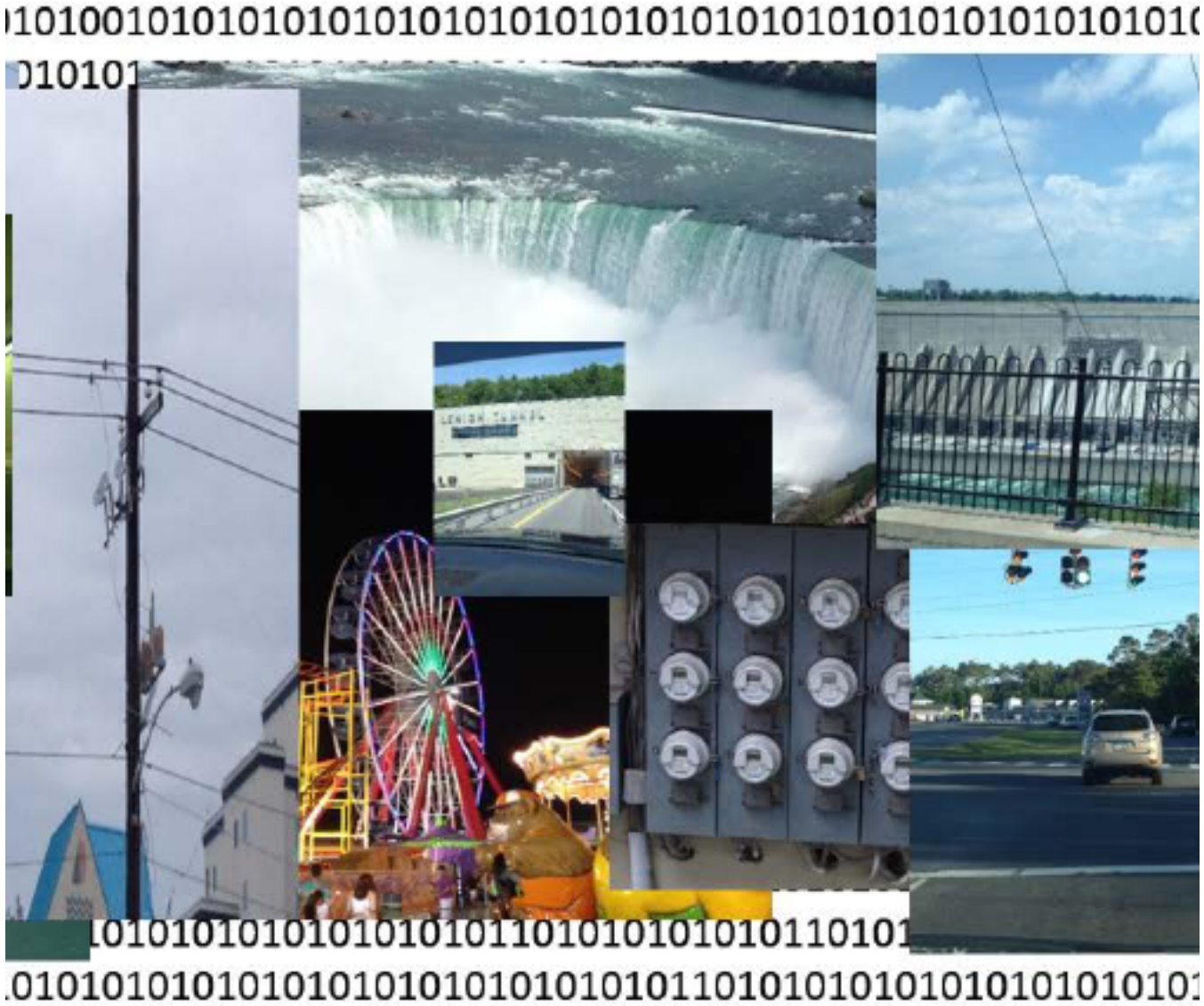


DES Mode	Type	IV	Error Propagation	Use case
Electronic Code Book (ECB)	Block	No	No	simplest form, weak, vulnerable to pattern attacks, good for small amounts data, least secure of all modes
Cipher Block Changing (CBC)	Block	Yes	Yes	Depends on cipher text from previous block to encrypt next block, uses chaining", creates propagation because the chaining, the IV creates a unique patter, each time
Cipher feedback mode (CFB)	**Stream**	Yes	yes	Very similar to CBC, but this is a, **stream,** not a block , data is encrypted in real time , the block is turned in the a "key stream generator"
Output Feedback mode (OFB)	Stream	yes	no	Just like CFM, **no error, propagation** because the Seed value is used before it becomes ciphertext, or the XOR is applied
Counter mode (CTR)	Stream	yes	no	Much like OFB, Instead of a seed, there is an IV, or **incremental counter,** each encryption step or plain text bock (packet) is done independent) – this ensures that each block is XORed with a unique keystream value, with no chaining – CTR mode Is often used to improve performance as well

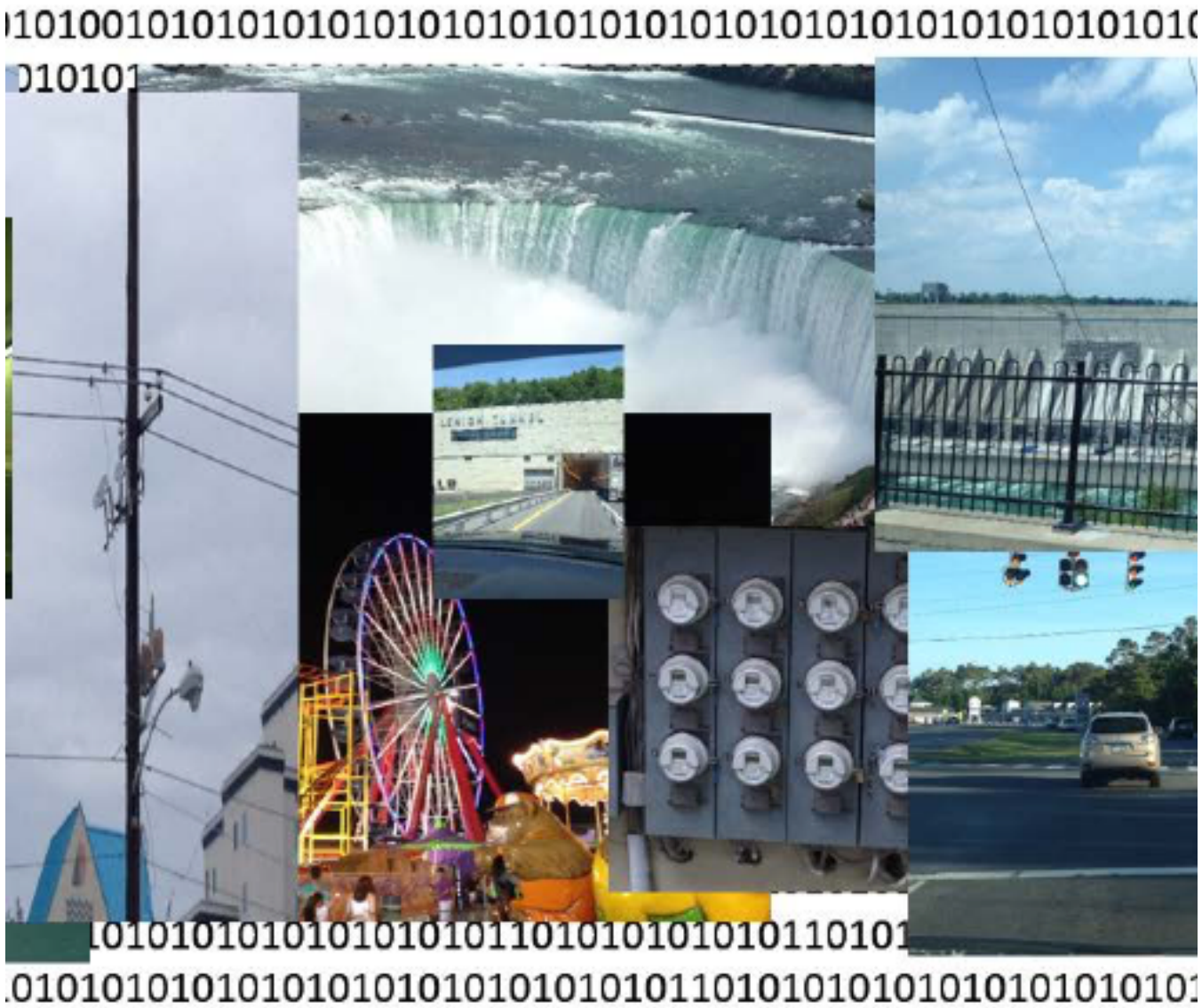
Advanced Symmetric Cryptography Concepts

DES

- Feistel function
- Splits the block on plain text in two two parts (LO and RO)
- The round function is applied to one of the halves
- The round functions is performed on one of the halves
- Details of each round vary with the mathematical operations of algorithm
- The output is then XOR'd with the other half
- This is done 16 times

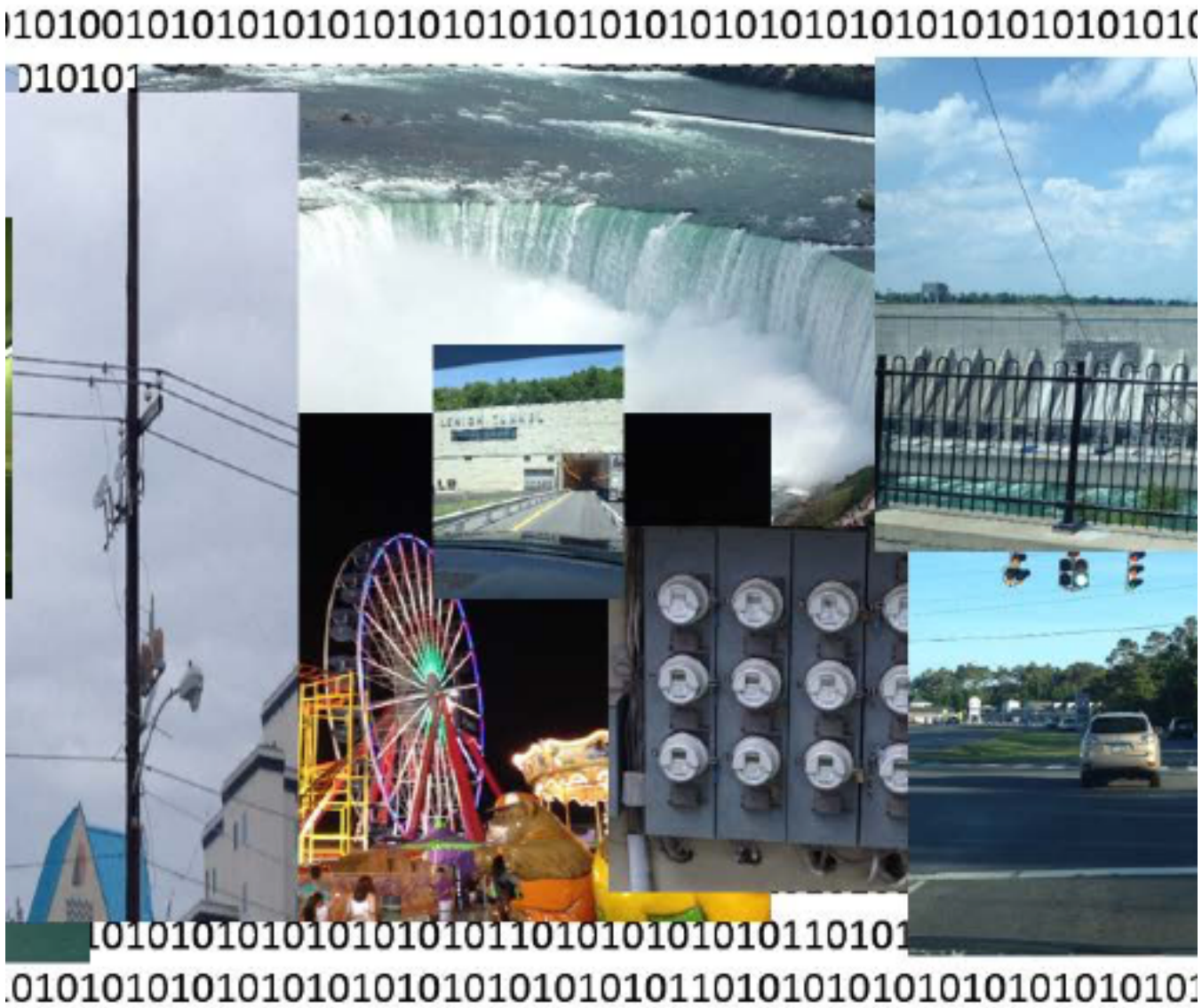


- Broke in 1998
- Tried 2 DES
- Led to 3DES
- The AES bord



Advanced Symmetric Cryptography

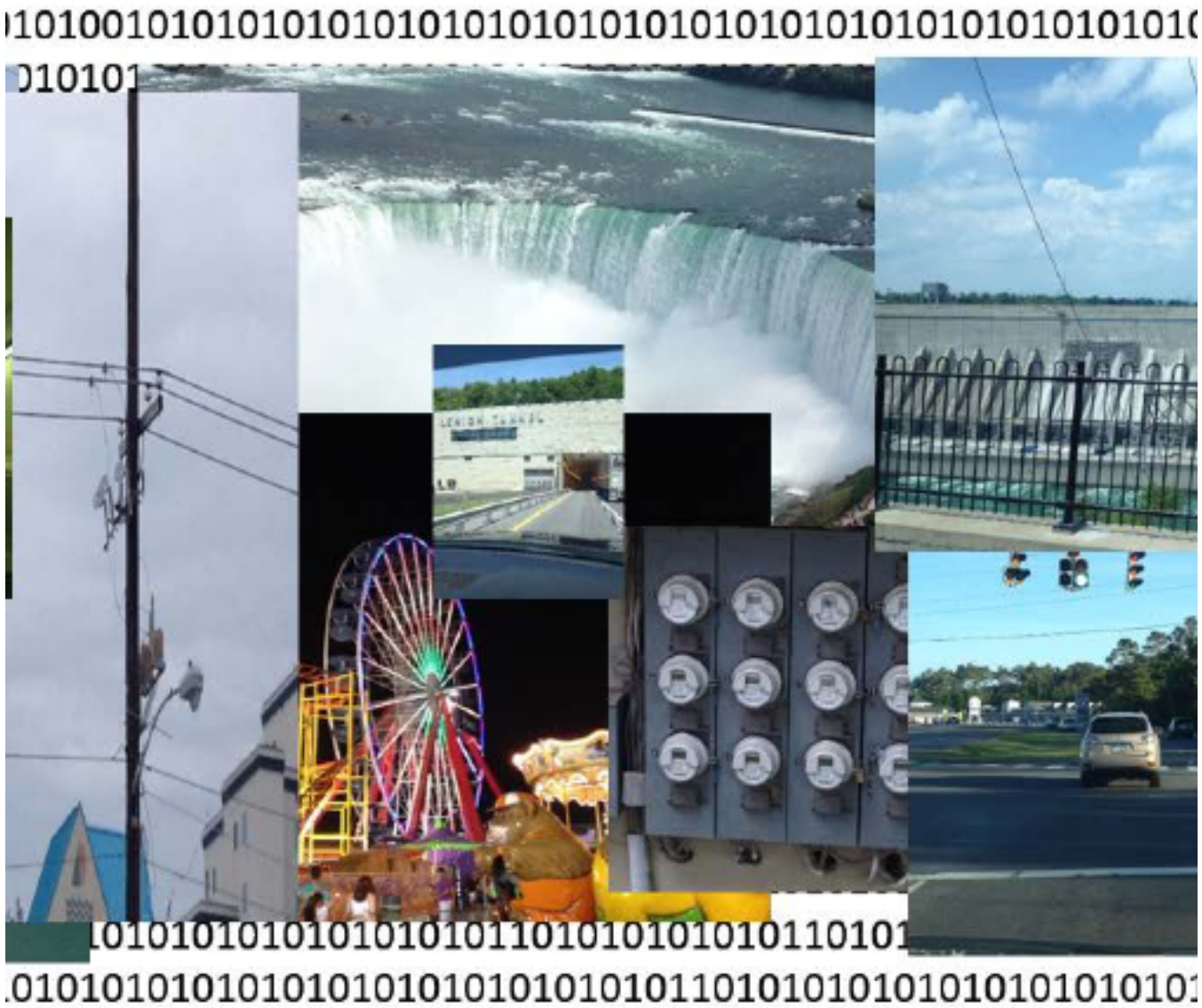
- DESx- “Key whitening”- XOR a key with the text before the round function, after, or both
- Extend DES
- Uses 48 rounds
- Four modes
  - DES EEE2
  - DES EDE2
  - DESEEE3
  - DES EDE3



Advanced Symmetric Cryptography Concepts

AES

- **Rijndael Block Cipher**
- **FIPS 197 Standard**
- **Substitution permutation matrix as oppose to the *Feistel Network , also referred to all a 4x4 Colum matrix state***
  - ***Key expansion***
  - ***Initial round round***
  - ***Rounds***
    - ***Sub bytes- each byte is replacing with another using a look up table***
    - ***Shift rows- transposition***
    - ***Mix columns***
    - ***Add round key***
  - ***Final Round***
    - ***Sub bytes***
    - ***Shift rows***
    - ***AddRoundKey***
- **10,12,14 rounds**
- **128, 192, 256-bit key size**
- **Block size 128**



Name	Block Size	Key size	Round	Structure
DES	64 bit	56 bit	16 Rounds	Feistel
3DES	64	168	48	Feistel
AES	128 bit	128,192,256 bit	10,12,14 rounds	Substitution-permutation matrix
Blowfish	64 bit	32-448 bit	16 rounds	Feistel
Twofish	128 bit	1-256	16 rounds	Feistel
Serpent	128	128,192,256	32 rounds	Substitution-permutation matrix
CAST	64	128, 256	12, 16 rounds	Feistel
Skipjack/Clipper Chip	64 bit	80 bit	32 rounds	Unbalanced Feistel
IDEAL	64 Bit	128 bit	8	Lai-Massey Scheme
TEA	64	128	64	Feistel
RC4	Stream	1-256		Key Stream- X-OR
RC5	32,64,128	2048	variable	
RC6	32,64,128	2048	variable	Speed improved RC4, AES competition
SHARK	64	128	6	Substitution-permutation matrix