

Cryptography 201



Agenda

- Review of Cryptography 101
- Warm up challenges
- Symmetric Encryption
 - DES
 - AES
- Asymmetric Encryption
 - RSA
- Wrap up

Importance of Cryptography

The background is a dark blue gradient. It features several glowing, translucent blue ribbons that spiral and twist across the frame, composed of binary digits (0s and 1s). In the center, there is a faint, light blue shield icon with a keyhole at the bottom, partially obscured by the ribbons.

1. **Confidentiality:** Ensure that the data can only be seen by the intended recipients.
2. **Integrity:** Ensure that the received data has not been altered or tampered with.
3. **Non-repudiation:** Ensure that the sender really did send the data.
4. **Authentication:** The process of proving one's identity.

Important Terms

Plaintext - Original text, readable by human beings, something that we can understand

Ciphertext - Text after it has been encrypted

Cipher - An algorithm/technique for performing encryption or decryption

Encryption - The process of converting plaintext into ciphertext

Decryption - The process of converting ciphertext back into plaintext

Important Terms

Keys - A string used in combination with a cipher (encryption algorithm) to transform plaintext into ciphertext, without knowing the key ciphertext cannot be converted back to plaintext

Key space - Number of possible keys that can be created from an algorithm, the larger the key space the more secure the algorithm

Encryption Algorithms

Kerckhoffs' Principle states that the security of a cryptosystem must lie in the choice of its keys only; everything else (including the algorithm itself) should be considered public knowledge.

An encryption algorithm is a mathematical formula used to transform data into meaningless ciphertext.

Use protocols and algorithms that are widely-used, heavily analyzed, and accepted as secure.


Longer the key size, the harder it is to brute force. However the larger the key size the more computing power is required.

Commonly used encryption algorithms include:

- DES
- AES - 128, 192, 256 bits in key size
- RSA

Block Cipher

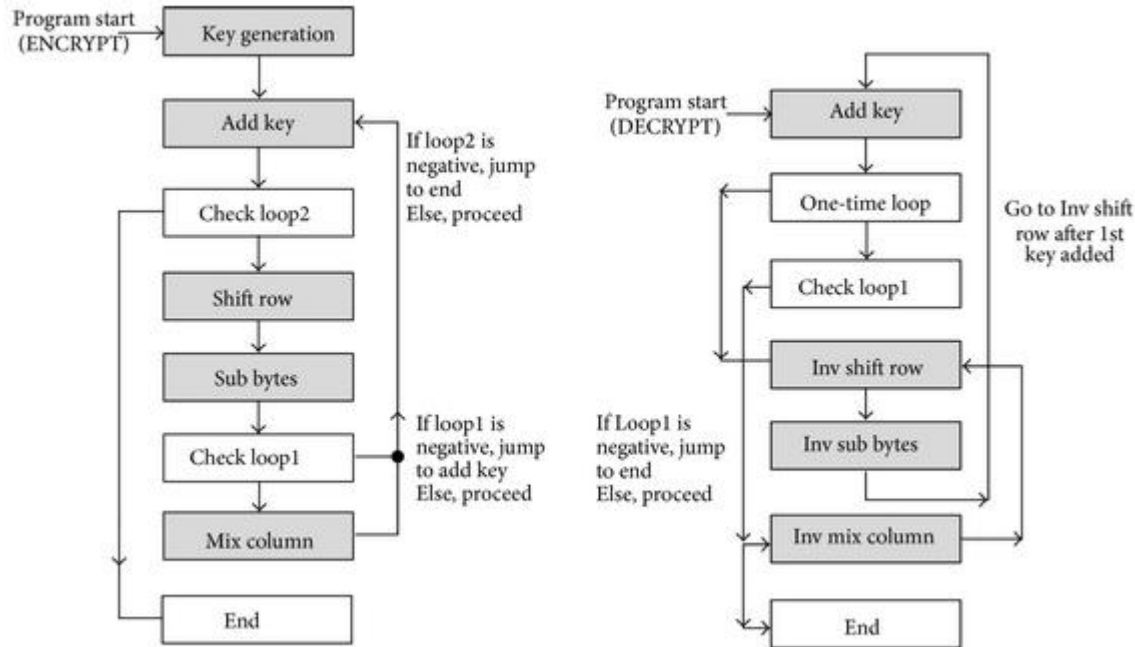
Encryption happens on a block of data

- 
- DES
 - 3DES
 - AES

Stream Cipher

Single bit of data is encrypted at a time

- 
- RC4
 - SEAL



Picture Source: Malwarebytes

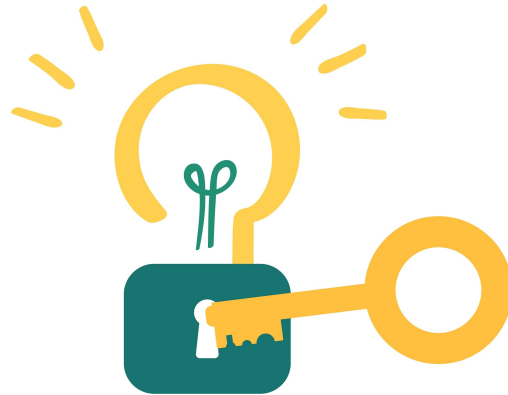
Encryption

Decryption

Plain text

Cipher text

Plain text



Encoding vs Encryption

- Encoding is the transformation of data from one form to another
- Useful for transmission of data, efficient storage of data
- Ex. Converting hexadecimal to ASCII is a form of encoding, convert message into morse code

Encryption is also the transformation of data from one form to another but an encryption algorithm is used alongside a key. If the key is unknown the message cannot be reversed.

Symmetric Encryption

- One key is used to encrypt plaintext and decrypt it as well
- The key is shared among the receiver and sender of data
- Key must be protected
- Ex. Caesar cipher, AES, DES



DES

- Data Encryption Standard
- Created in 1974 by IBM, adopted by NIST
- DES has an effective key length of 56 bits
- Overtime it was discovered that DES was a weak algorithm because it's 56-bit key is too short
- "The only solution here is to pick an algorithm with a longer key; there isn't enough silicon in the galaxy or enough time before the sun burns out to brute-force triple-DES" (*Crypto-Gram*, Counterpane Systems, August 15, 1998)
- Triple DES systems are significantly more secure than single DES
- Triple DES applies the DES cipher in triplicate

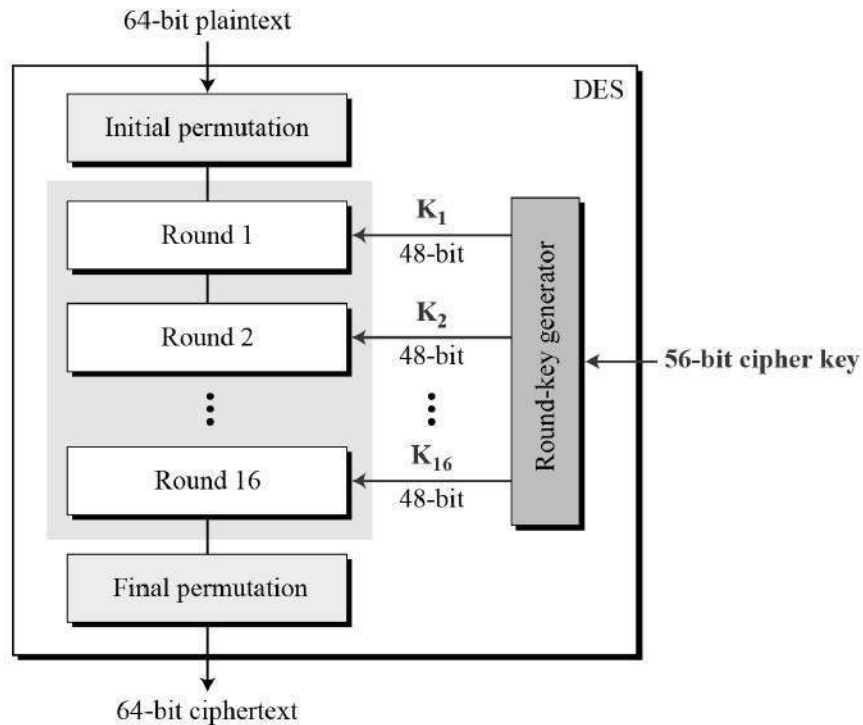


Image source :
https://www.tutorialspoint.com/cryptography/data_encryption_standard.htm

AES

- Advanced Encryption Standard
- AES encryption has three different block ciphers: AES-128 (128 bit), AES-192 (192 bit) and AES-256 (256 bit). These block ciphers are named after the key length they use for encryption and decryption. All these ciphers encrypt and decrypt the data in 128-bit blocks but they use different sizes of cryptographic keys.
- Since the AES algorithm is considered secure, it is in the worldwide standard.
- There are three options for encryption key lengths: 128-, 192-, or 256-bits.



Asymmetric Encryption

- Also known as ‘public key cryptography’
- Involves a key pair that are mathematically connected and work in conjunction with each other
- Private key, public key (Key pair)
- The sender uses the receiver's Public key to encrypt the data and the private key is used by the receiver to decrypt the message.
- Ex. RSA, ECC, El Gamal



RSA

- Asymmetric cryptosystem
- In 1977, Ron Rivest, Adi Shamir, and Leonard Adleman (Inventors of RSA) publicly described the algorithm.
- A public-key algorithm that is used for key establishment and the generation and verification of digital signatures. (NIST)

How does RSA work?

1. Privately select two large prime numbers, P and Q . If someone gains access to these, then you are vulnerable to attack.
2. Multiply the two numbers to create $n = P \times Q$. This is your public key.
3. Calculate $\Phi(n)$ such that $\Phi(n) = (P - 1) \times (Q - 1)$.
4. Choose a number, e , such that $1 < e < \Phi(n)$.
5. Your total public key is (n, e) .
6. Calculate $d = (k \cdot \Phi(n) + 1) / e$ for some integer k . d is your private key!
7. Your total private key is (n, d) . To send a message m , the other person needs to calculate $x = m^e \pmod n$ and send x to you. This is the encrypted message.

Now you decrypt it by calculating $x^d \pmod n$. This will give you back the original message m . The best way to use this algorithm is for the other person to sign the message with your public key and his own private key to ensure Authenticity and Encryption.

How does RSA work?

RSA public key: Is a pair of numbers (e,n)

RSA private key: Is a pair of numbers (d,n)

Message: m

Ciphertext: c

To encrypt: $m^e \bmod n = c$

To decrypt: $c^d \bmod n = m$

Public key $(e,n) \rightarrow (11,117)$

Private key $(d,n) \rightarrow (35,117)$

Message $m \rightarrow 10$

So far, we have a private key which has an $e=11$, and a public key with a $d=35$. Our message is 10. To encrypt 10, we do:

$$10^{11} \bmod 117$$

The result of that is 82. So, we have:

$$10^{11} \bmod 117 = 82$$

Ciphertext $\rightarrow 82$

Now, for decrypting, we do:

$$82^{35} \bmod 117 = 10$$

Cleartext $\rightarrow 10$

To encrypt: $m^e \bmod n = c$

To decrypt: $c^d \bmod n = m$

Resources

Resource Hub available at <https://dmz.ryerson.ca/canhack/>

PicoCTF primer available at <https://picoctf.org>

Scripts:

https://en.wikibooks.org/wiki/Algorithm_Implementation/Mathematics/Extended_Euclidean_algorithm

RSA Cryptography: <https://www.geeksforgeeks.org/rsa-algorithm-cryptography/>

Online Tools for encrypting/decrypting:

<https://cryptii.com/>

<https://gchq.github.io/CyberChef/>

Thank you for your time!

Questions?

See you next week for Digital Forensics 201!

