

# Ciphers: How Malware's Keep Their Secrets Safe

Stars of the Malware Cipher Show: AES, DES, RC4, Salsa20, 3DES, Serpent.

Muhammad Ahmad

[Kill\_The\_Malware]

# Malware Families using Symmetric Encryption











- RC4 is a **stream cipher** that is no longer considered to be secure. It was designed by Ron Rivest in 1987 and is a variable-key-length cipher, which means that the key can be any length from 64 bits to 256 bits.

Encryption Algorithm	Malware families	Category
RC4	Dridex	Baking Trojan 🐔
RC4	IceDid	Baking Trojan 🐔
RC4	Panda Banker	Baking Trojan 🐔
RC4	TrickBot	Modular Trojan 🐔
RC4	Agent Tesla	Remote access trojan 🐔
RC4	GandCrab	Ransomware 💀
RC4	Turla PowerShell Loader	Loader 📁
RC4	Ramnit	Baking Trojan 🐔
RC4	WannaCry	Ransomware 💀
RC4	Phobos	Ransomware 💀
RC4	Petya	Ransomware 💀
RC4	Angler Exploit Kit	Exploit kit 🏠

# Malware Families using Symmetric Encryption




**AES (Advanced Encryption Standard):** A **block cipher** using fixed-size blocks, replacing the older DES, AES employs complex substitution and permutation operations to securely transform data.

**Salsa20:** A **stream cipher** designed for efficient and secure data encryption, involving various operations like addition, rotation, and mixing to generate the encrypted output.

Encryption Algorithm	Malware families	Category
AES-128	WannaCry	Ransomware 
AES-128	Petya	Ransomware 
AES-256	Ryuk	Ransomware 
AES-128	Emotet	Trojan 
AES-128	TrickBot	Trojan 
Salsa20	GandCrab	Ransomware 
Salsa20	Revil	
Salsa20	Sodinokibi	Ransomware 
Salsa20	DarkSide	Ransomware 
Salsa20	Conti	Ransomware 







# Malware Families using Symmetric Encryption

- **3DES (Triple Data Encryption Standard):** is **block cipher** Enhancing security over DES, 3DES applies the DES algorithm three times consecutively to each data block, using two or three different keys.
- **Serpent:** A strong **block cipher** known for its security, Serpent employs multiple rounds of substitutions, permutations, and mixing to encrypt data thoroughly.

Encryption Algorithm	Malware families	Category
3DES	ISFB	Banking trojan 
3 DES	WannaCry	Ransomware 
Serpent	ISFB	Banking trojan 

## Malware families using A Symmetric Encryption

- **ECDH (Elliptic Curve Diffie-Hellman):** A key exchange technique using elliptic curve cryptography to securely share secret keys over a public channel, based on the mathematical properties of elliptic curves.
- **RSA (Rivest-Shamir-Adleman) :** An asymmetric encryption algorithm that employs a pair of keys, a public key for encryption and a private key for decryption, relying on the difficulty of factoring large semiprime numbers for its security.

Encryption Algorithm	Malware families	Category
ECDH	Petya	Ransomware 
ECDH	Angler Exploit Kit	Exploit Kit 
RSA	WannaCry	Ransomware 
RSA	ISFB	Banking Trojan 
RSA	Emotet	Banking Trojan 
RSA	Phobos	Ransomware 

# References

## RC4

<https://www.appgate.com/blog/reverse-engineering-dridex-and-automating-ioc-extraction>  
<https://www.malwarebytes.com/blog/news/2019/12/new-version-of-icedid-trojan-uses-steganographic-payloads>  
<https://www.spamhaus.org/news/article/771/pandaze-uss-christmas-gift-change-in-the-encryption-scheme>  
<https://blog.cloudflare.com/trickbot-spear-phishing-drops-malware/>  
<https://trojan-killer.net/the-famous-infostealer-agent-tesla-has-an-unusual-dropper/>  
<https://www.acronis.com/en-gb/blog/posts/gandcrab/>  
<https://cybersecuritynews.com/new-turla-crutch-backdoor/>  
<https://cert.pl/en/posts/2017/09/ramnit-in-depth-analysis/>  
[https://www.trendmicro.com/en\\_gb/research/17/e/wannacry-uwix-ransomware-monero-mining-malware-follow-suit.html](https://www.trendmicro.com/en_gb/research/17/e/wannacry-uwix-ransomware-monero-mining-malware-follow-suit.html)  
<https://medium.com/@danielsharon278/phobos-ransomware-campaign-in-middle-east-6fb38308c79>  
<https://resources.infosecinstitute.com/topics/cryptography/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/>  
<https://unit42.paloaltonetworks.com/unit42-understanding-angler-exploit-kit-part-1-exploit-kit-fundamentals/>

## AES

<https://www.mandiant.com/resources/blog/wannacry-malware-profile>  
<https://www.crowdstrike.com/blog/petrwrap-ransomware-technical-analysis-triple-threat-file-encryption-mft-encryption-credential-theft/>  
<https://www.extrahop.com/company/blog/2020/ransomware-explanation-and-prevention/>  
<https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-emolets-use-of-cryptography/>  
<https://www.vmray.com/cyber-security-blog/malware-analysis-spotlight-emolets-use-of-cryptography/>

## Salsa-20

<https://www.trellix.com/ja-jp/about/newsroom/stories/research/gandcrab-ransomware-puts-the-pinch-on-victims.html>  
<https://securelist.com/revil-ransomware-attack-on-msp-companies/103075/>  
<https://www.acronis.com/en-gb/blog/posts/sodinokili-ransomware/>  
<https://www.key.sight.com/blogs/tech/news/2021/05/18/darkside-ransomware-behavior-and-techniques>  
<https://www.key.sight.com/blogs/tech/news/2021/05/18/darkside-ransomware-behavior-and-techniques>

## 3DES

<https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/>

## Serpent

<https://www.welivesecurity.com/2019/05/29/turla-powershell-usage/>  
<https://www.sentinelone.com/labs/writing-malware-traffic-decrypters-for-isfb-ursnif/>

## ECDH

<https://resources.infosecinstitute.com/topics/cryptography/a-brief-summary-of-encryption-method-used-in-widespread-ransomware/>

## RSA

<https://www.secureworks.com/research/wcry-ransomware-analysis>  
<https://www.sentinelone.com/labs/writing-malware-traffic-decrypters-for-isfb-ursnif/>  
<https://cert.pl/en/posts/2020/02/whats-up-emolet/>  
<https://www.malwarebytes.com/blog/news/2020/01/threat-spotlight-phobos-ransomware-lives-up-to-its-name>