IERG 4998 Final Year Project I Presentation

Group C1 Encrypted Cloud Storage for smartphones

Supervisor: CHAU, Sze Yiu

Name: IP Shing On SID: 1155109011

Name: WONG Shing SID: 1155109027

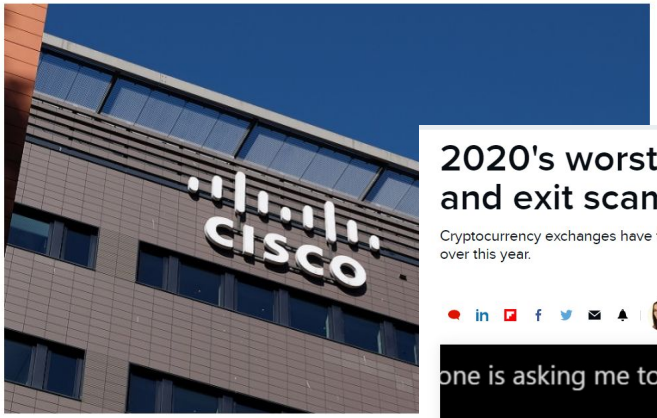
Background

Ex-Cisco Engineer Pleads Guilty in Insider Threat Case

Sudhish Kasaba Ramesh Caused $1.4 Million in Damages to Former Employer

Scott Ferguson (@Ferguson_Writes) · August 29, 2020

Twitter Facebook LinkedIn Credit Eligible Get Permission



A former Cisco engineer has pleaded guilty to causing $1.4 r

EDITORS' PICK | 238,366 views | Jan 22, 2020, 06:10am EST

Microsoft Security Shocker As 250 Million Customer Records Exposed Online

Davey Winder Senior Contributor

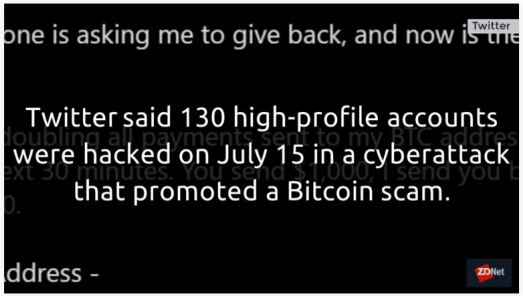
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

2020's worst cryptocurrency breaches, thefts, and exit scams

Cryptocurrency exchanges have felt the impact of everything from vulnerability exploit to social engineering scams over this year.

By Charlie Osborne for Zero Day | December 1, 2020 -- 09:00 GMT (17:00 SGT) | Topic: Security



MORE FROM CHARLIE OSBORNE

Holiday Gifts
Buy two: Tech gifts and gadgets so cool you'll want one for yourself too

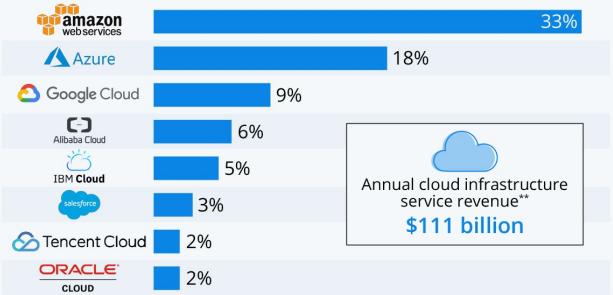
Innovation
Warner Bros to movie theaters: Drop dead

Security
The best gifts for hackers

Blockchain
Ripple CTO says community could

Amazon Leads $100 Billion Cloud Market

Worldwide market share of leading cloud infrastructure service providers in Q2 2020*



* includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

** 12 months ended June 30, 2020

Source: Synergy Research Group

statista

Encrypted Cloud Storage for smartphones

Cloud privacy problems	**Solutions**
Lack of End-to-end encryption	ChaCha20- Poly1305 AEAD ECC (Elliptic-curve cryptography)
No back-up system	main storage and backup storage
Not user friendly	PBKDF2

Boxycryptor - existing app

Symmetric key encryption:

AES-256, CBC mode, PKCS7 Padding

Attacks:

Lucky 13, Power Analysis Attack

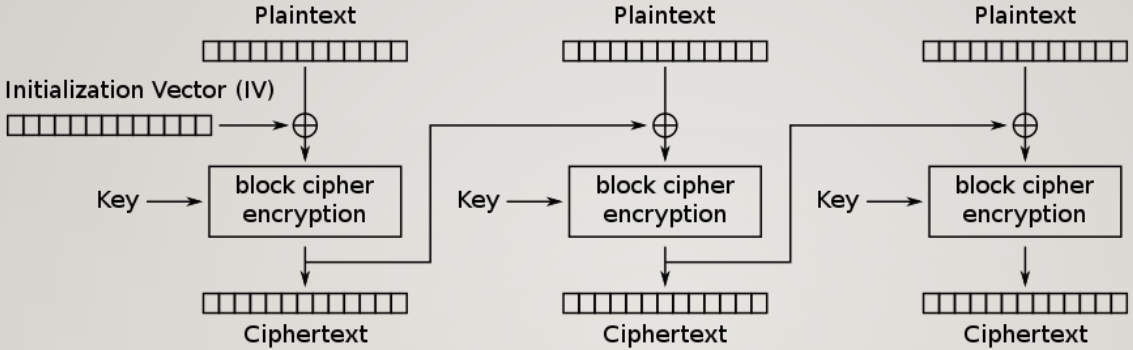
Asymmetric key encryption:

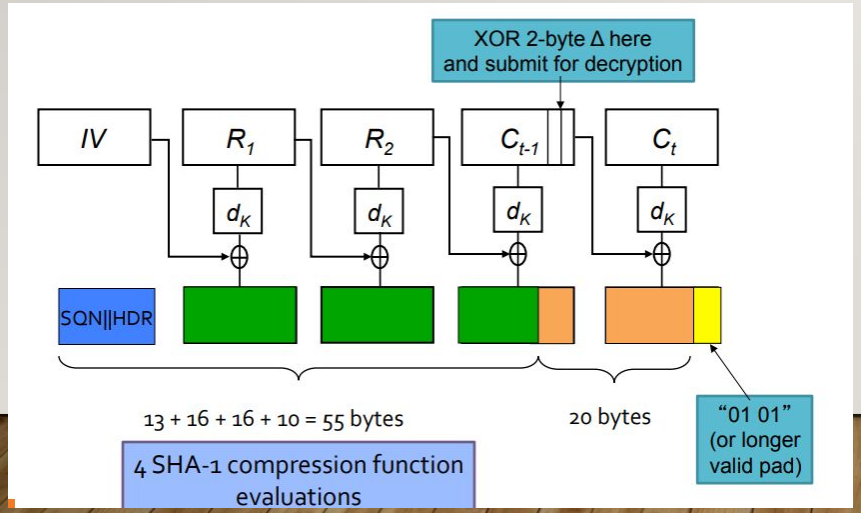
RSA OAEP

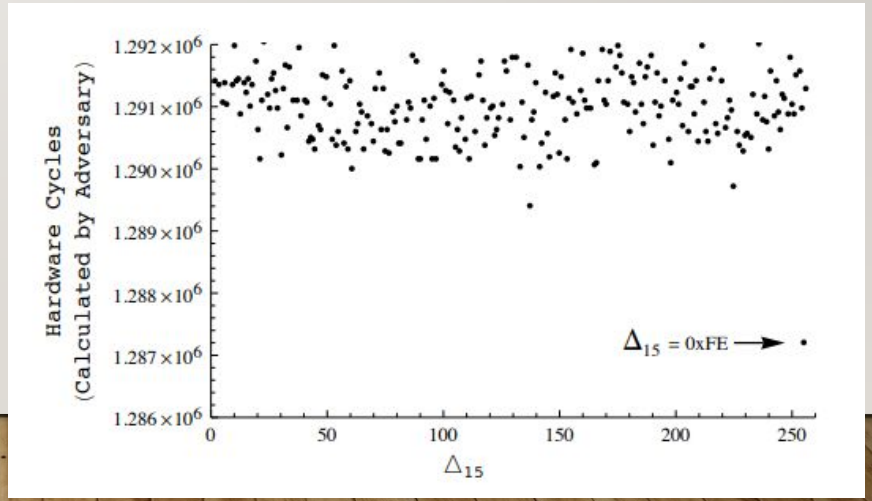
Attacks:

Side-channel attack, CCA2

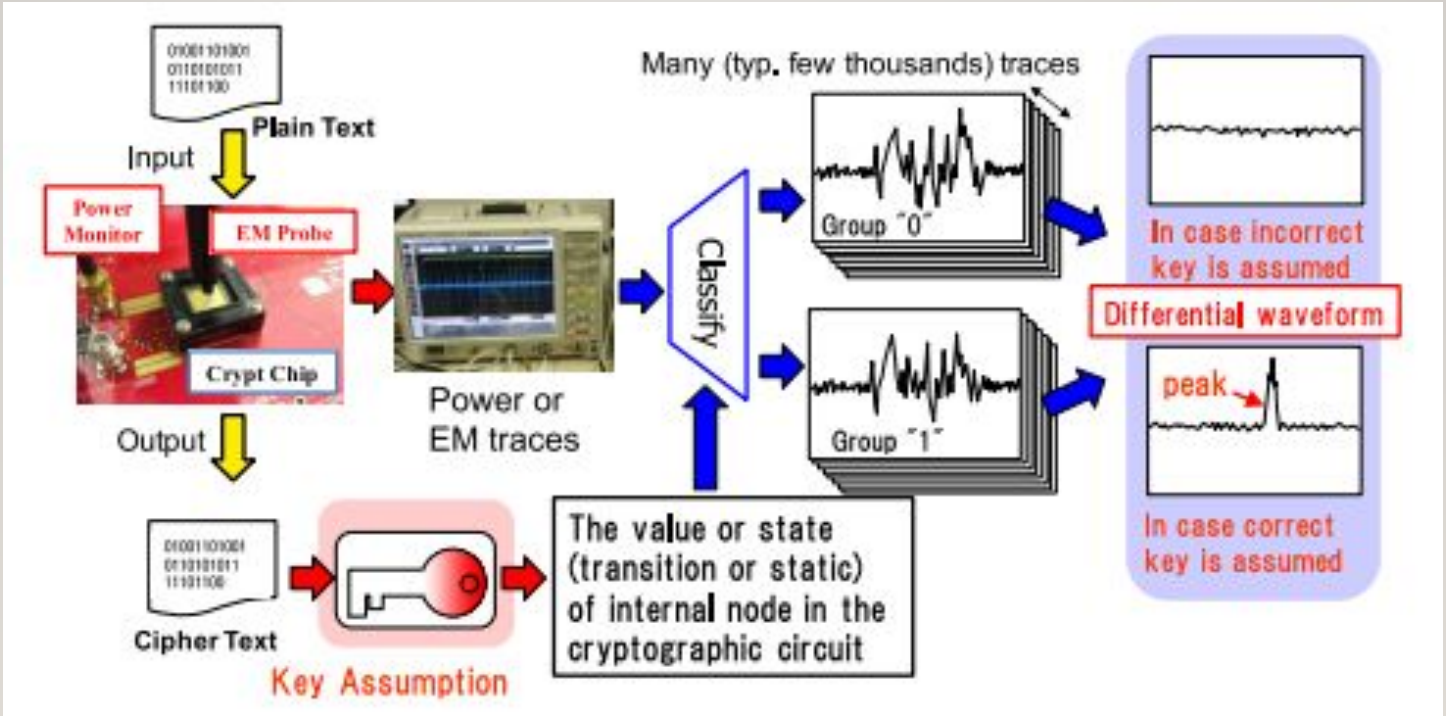
Lucky 13 (AES, CBC mode, PKCS7 padding)



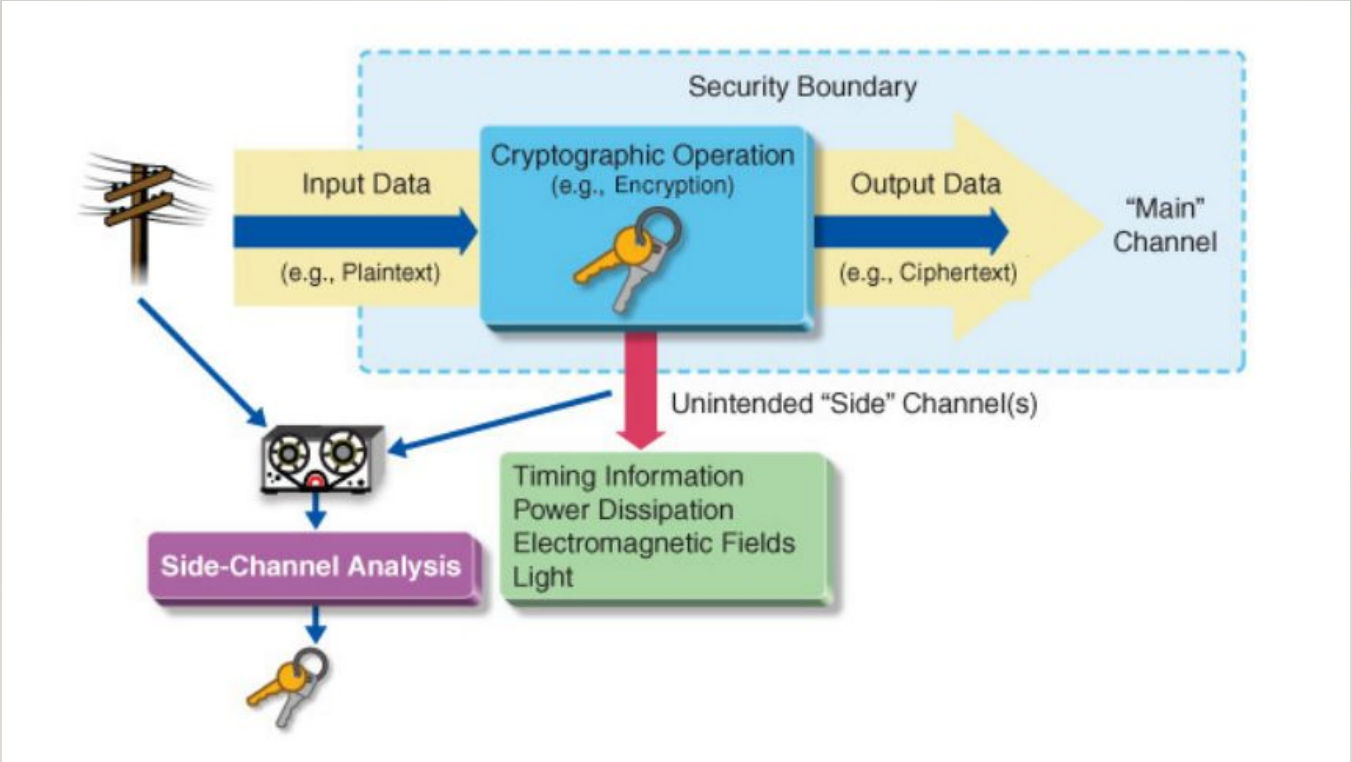




Power Analysis Attack



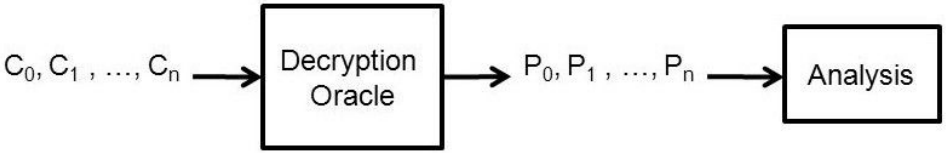
Side-channel Attack



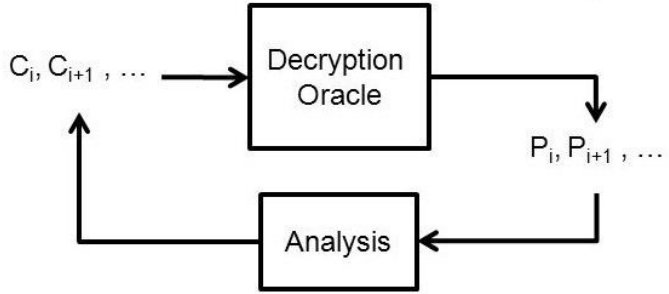
Adaptive Chosen Ciphertext Attack

Chosen Ciphertext Attack (CCA)

- **CCA1 : Lunchtime attack**



- **CCA2 : Adaptive Chosen Ciphertext Attack**



Methodology

ChaCha20-Poly1305 AEAD

ChaCha20: encryption Poly1305: authentication

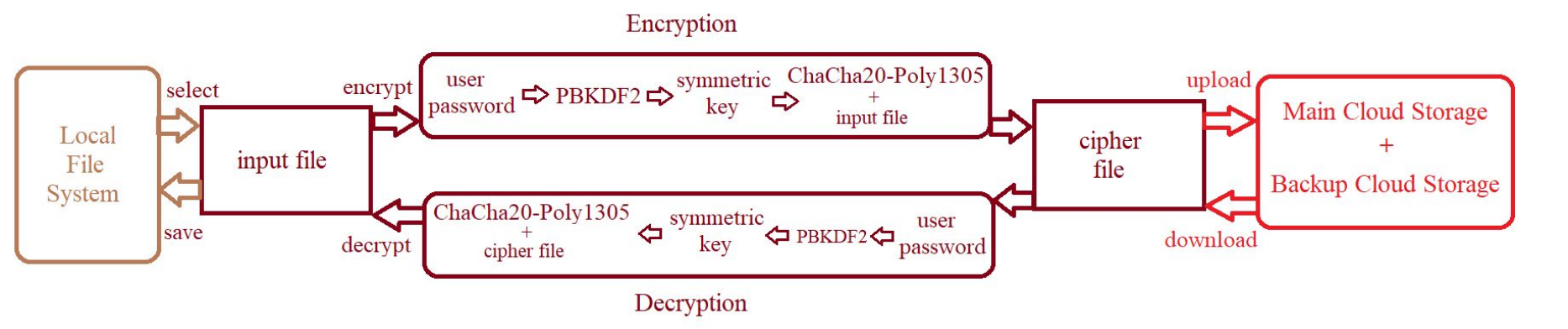
AEAD (authenticated encryption with additional data)

ECC (Elliptic-curve cryptography)

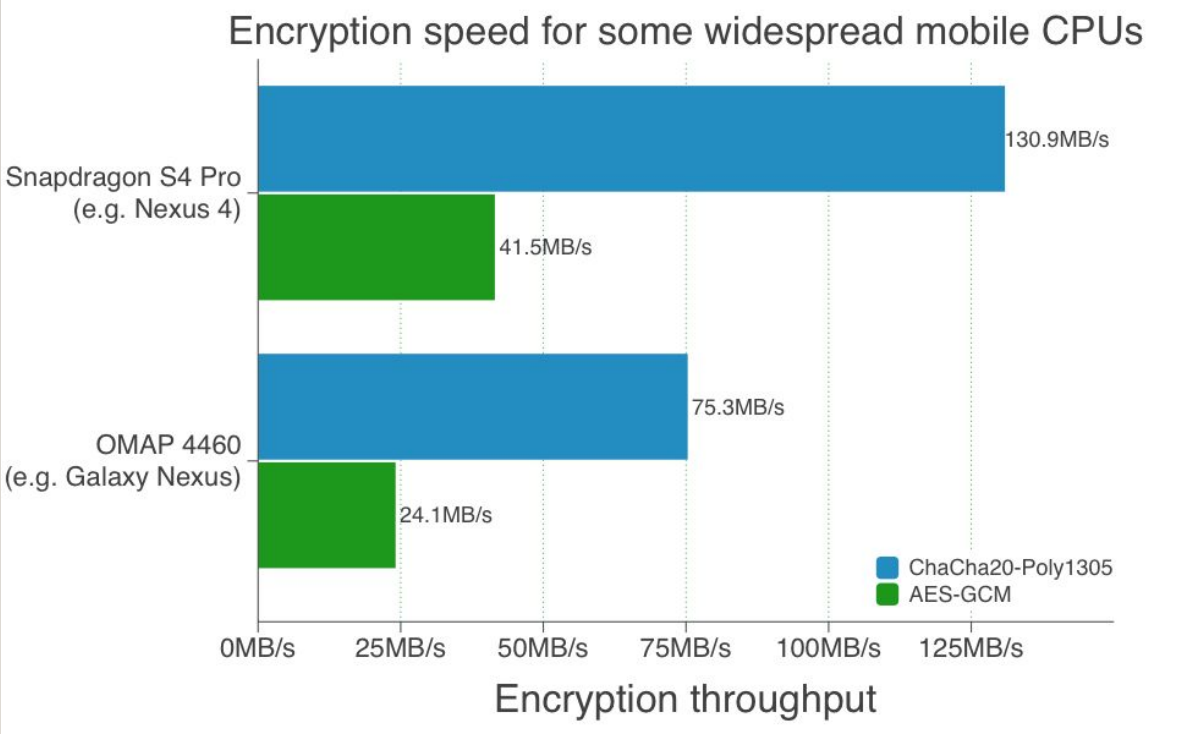
Difficulty of ECDLP (Elliptic Curve Discrete Logarithm Problem)

Key Exchange: ECDH (Elliptic Curve Diffie-Hellman Key Exchange)

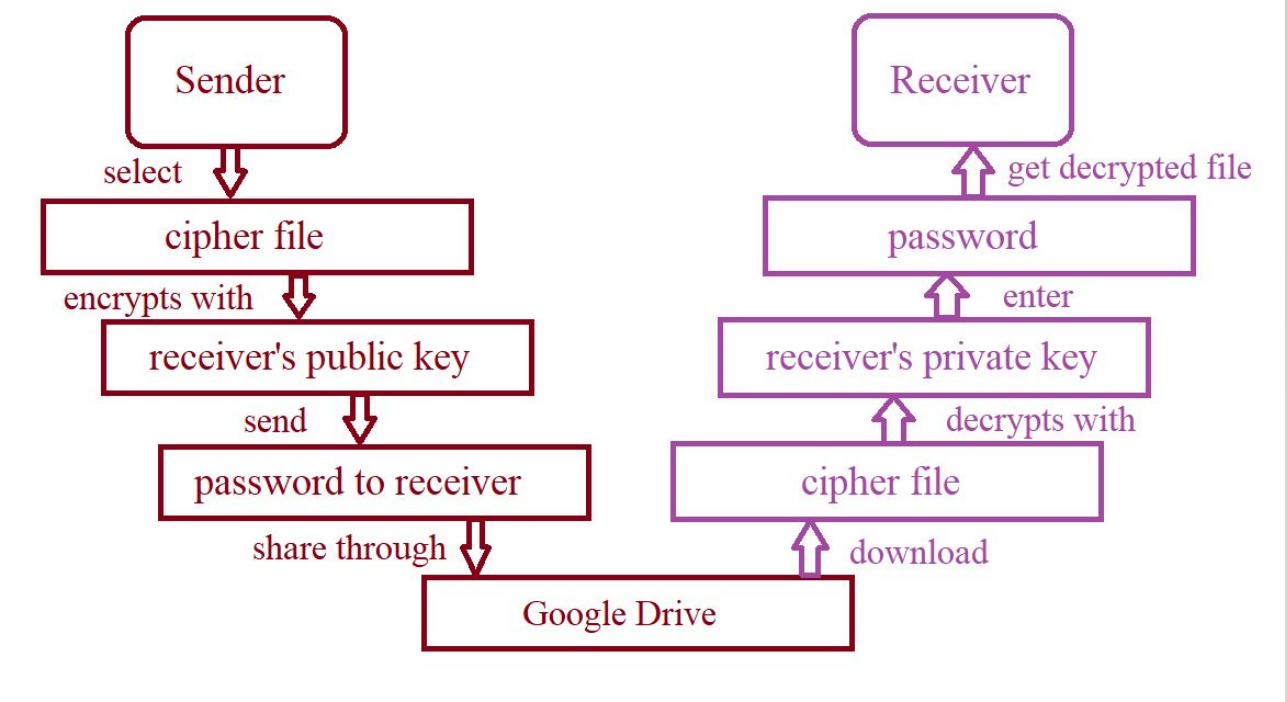
Files Encryption



ChaCha20-Poly1305 AEAD vs AES-GCM



Files Sharing



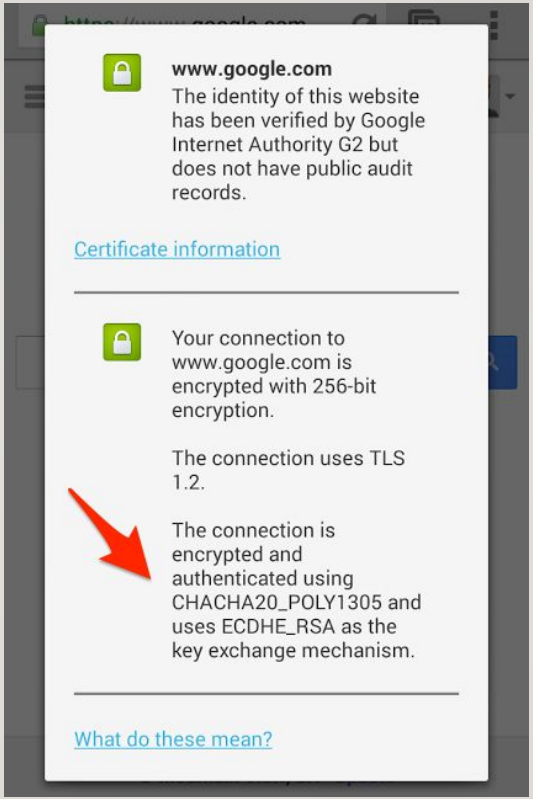
ECC vs RSA

Key Length		Time (s)	
RSA	ECC	RSA	ECC
1024	163	0.16	0.08
2240	233	7.47	0.18
3072	283	9.80	0.27
7680	409	133.90	0.64
15360	571	679.06	1.44

TABLE IV
256 BITS ENCRYPTION, DECRYPTION AND TOTAL TIME (IN SECONDS)

Security	Encryption		Decryption		Total	
Bits	ECC	RSA	ECC	RSA	ECC	RSA
80	7.92	0.55	22.88	19.31	30.80	19.87
112	39.70	0.58	26.33	102.03	66.03	102.61
128	58.43	0.56	27.40	209.60	85.84	210.17
144	77.50	0.57	32.15	311.06	109.65	311.63

Practicability

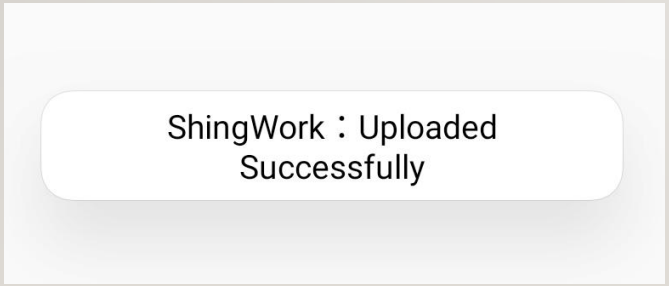


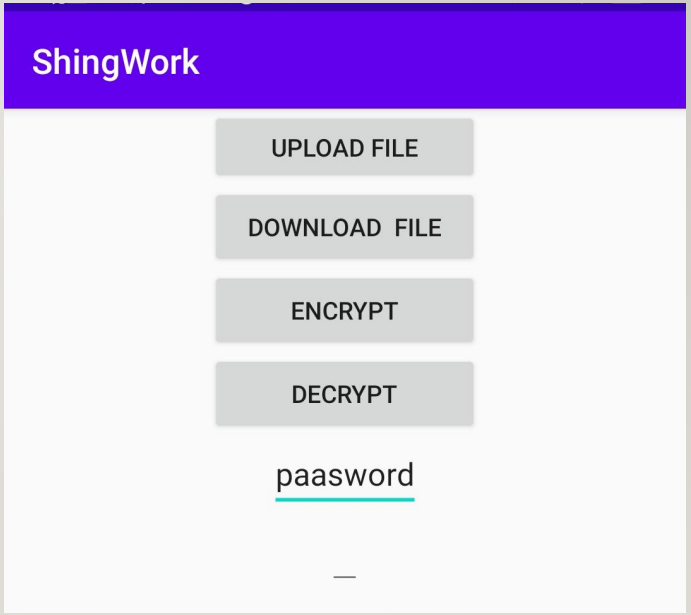
Implementations

1. Google Login

Implementations

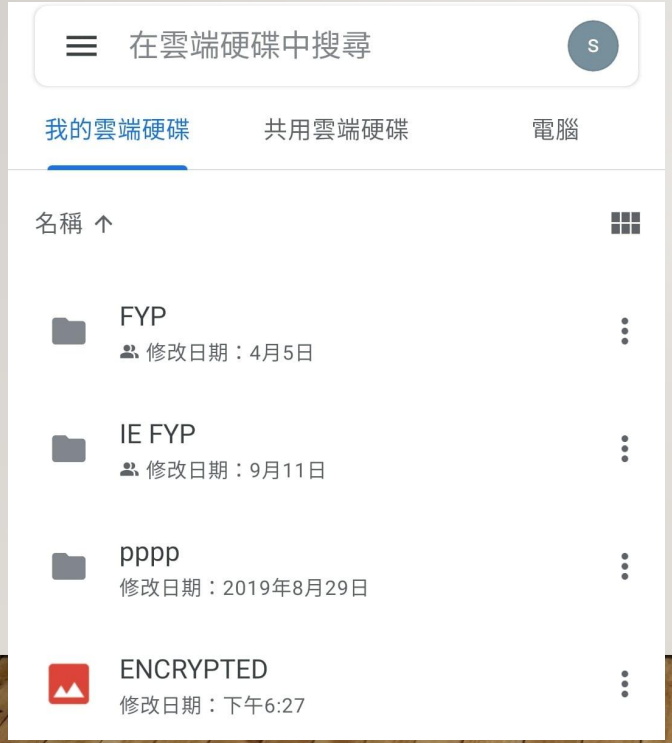
2. Select, Encrypt and Upload

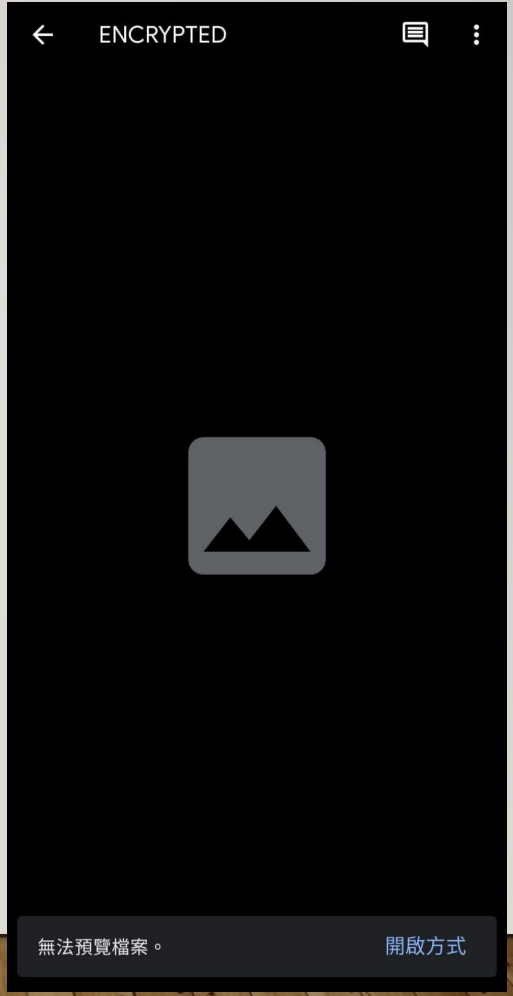




Implementations

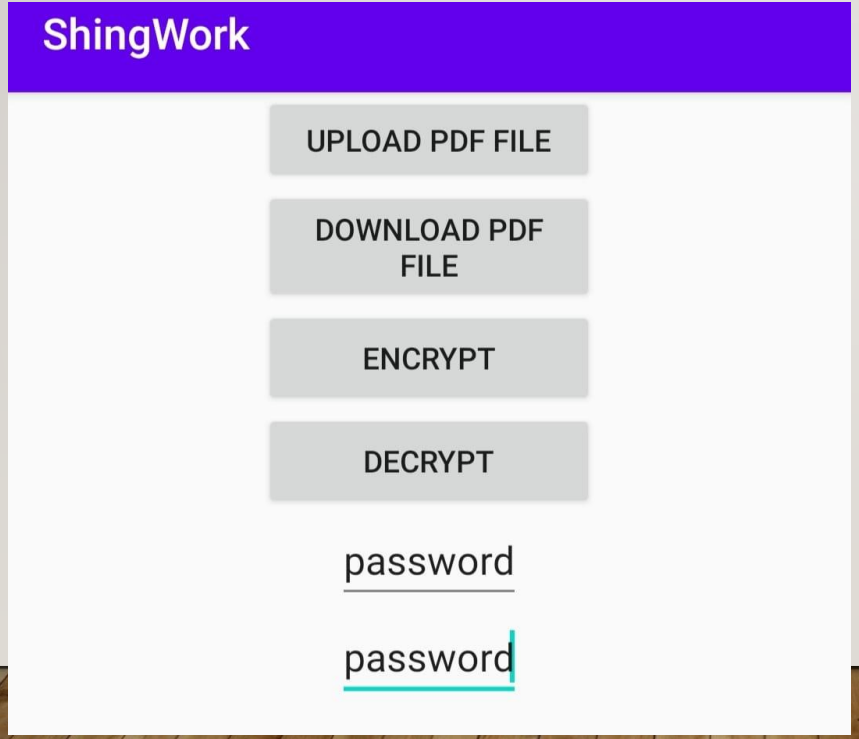
3. Check on the Google Drive

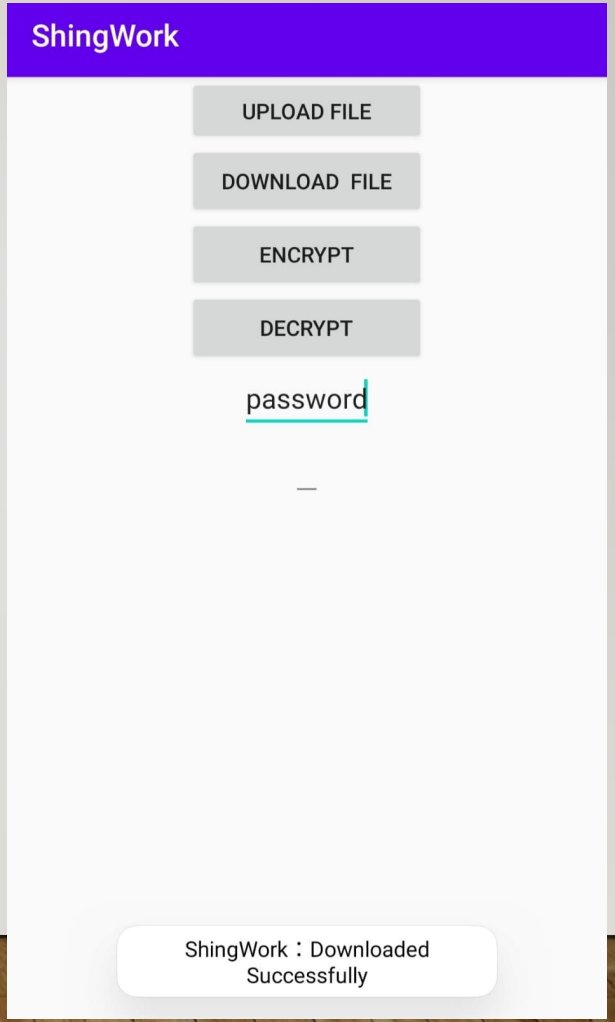




Implementations

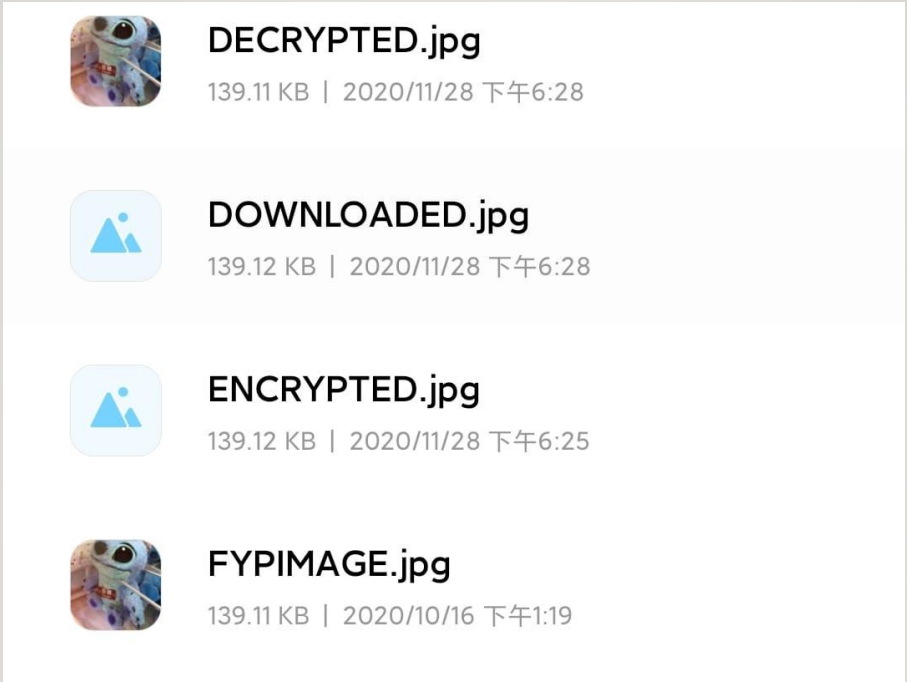
4. Decrypt and Download





Implementations

5. Check the files on the Loacl File System

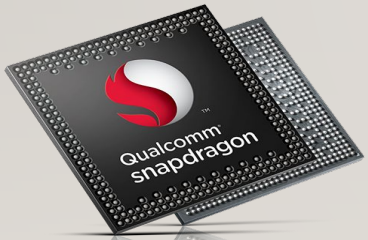


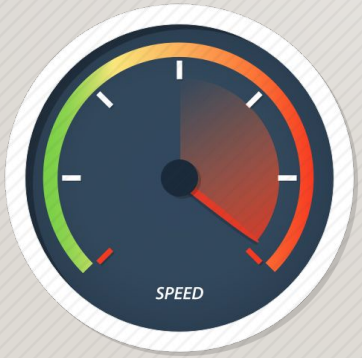
Evaluation

Performance (Speed)

throughput of

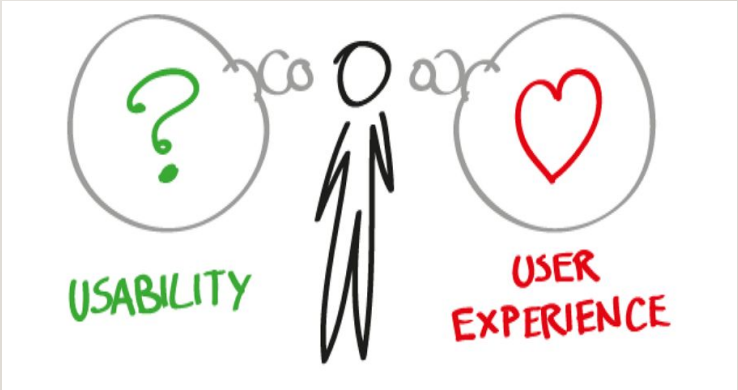
different input file size, CPUs





Usability

ease of selecting, encrypting, decrypting, sharing files



Future Work

1. ChaCha20-Poly1305 AEAD (File Selection)
2. ECC
3. Backup Cloud Storage
4. User Interface
5. App Design

Conslusion

- additional protection
- full control from the user
- Better Security
- Faster Speed
- Backup Cloud Storage

Confidentiality, Integrity and Availability

Reference

1. “Block cipher mode of operation,” *Wikipedia*, 30-Nov-2020. [Online]. Available: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation. [Accessed: 06-Dec-2020].
2. c0D3M, “Lucky 13 Attack Explained,” *Medium*, 10-Oct-2019. [Online]. Available: https://medium.com/@c0D3M/lucky-13-attack-explained-dd9a9fd42fa6. [Accessed: 06-Dec-2020].
3. N. J. Al Fardan and K. G. Paterson, "Lucky Thirteen: Breaking the TLS and DTLS Record Protocols," 2013 IEEE Symposium on Security and Privacy, Berkeley, CA, 2013, pp. 526-540, doi: 10.1109/SP.2013.42.
4. T. Fujino, T. Kubota, and M. Shiozaki, “Tamper-resistant cryptographic hardware,” *IEICE Electronics Express*, vol. 14, no. 2, pp. 20162004–20162004, 2017.
5. H. Gamaarachchi and H. Ganegoda, “Power Analysis Based Side Channel Attack.” [Online]. Available: https://www.researchgate.net/profile/Harsha_Ganegoda/publication/322243368_Power_Analysis_Based_Side_Channel_Attack/links/5a996e13aca2721e3f2db805/Power-Analysis-Based-Side-Channel-Attack.pdf.
6. P. Nadeeshani, “Vulnerability impact of RSA OAEP and PKCS#1 v1.5,” *Medium*, 31-Mar-2019. [Online]. Available: https://medium.com/@nshani/vulnerability-impact-of-rsa-oaep-and-pkcs-1-v1-5-924692befa71. [Accessed: 06-Dec-2020].