Cryptosystems for Mobile Devices

S. Dhanya Abhirami

66%

Of world population have mobile phone worldwide.

(As of July 2019)

Limitations in mobile ecosystem

- **Computational Limitations**

  Brute Force attacks are much easier on mobile phones than non-mobile counterparts

- **Power Limitations**

  Mobile devices are in use whole day long. So security application must not be responsible for draining of battery.

“Demand for computationally cheap, but still secure, cryptosystem rises”

- Prof. Ariel Hamlin

Elliptic Curve Cryptography

Overview

- ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields
- It requires smaller keys compared to non-EC cryptography to provide equivalent security..

Elliptic Curve Diffie Hellman (ECDH)

Public Information:

i. Elliptic Curve:

- Coefficients a and b
- p, a large prime

ii. Point P on Elliptic Curve, whose order is large value n

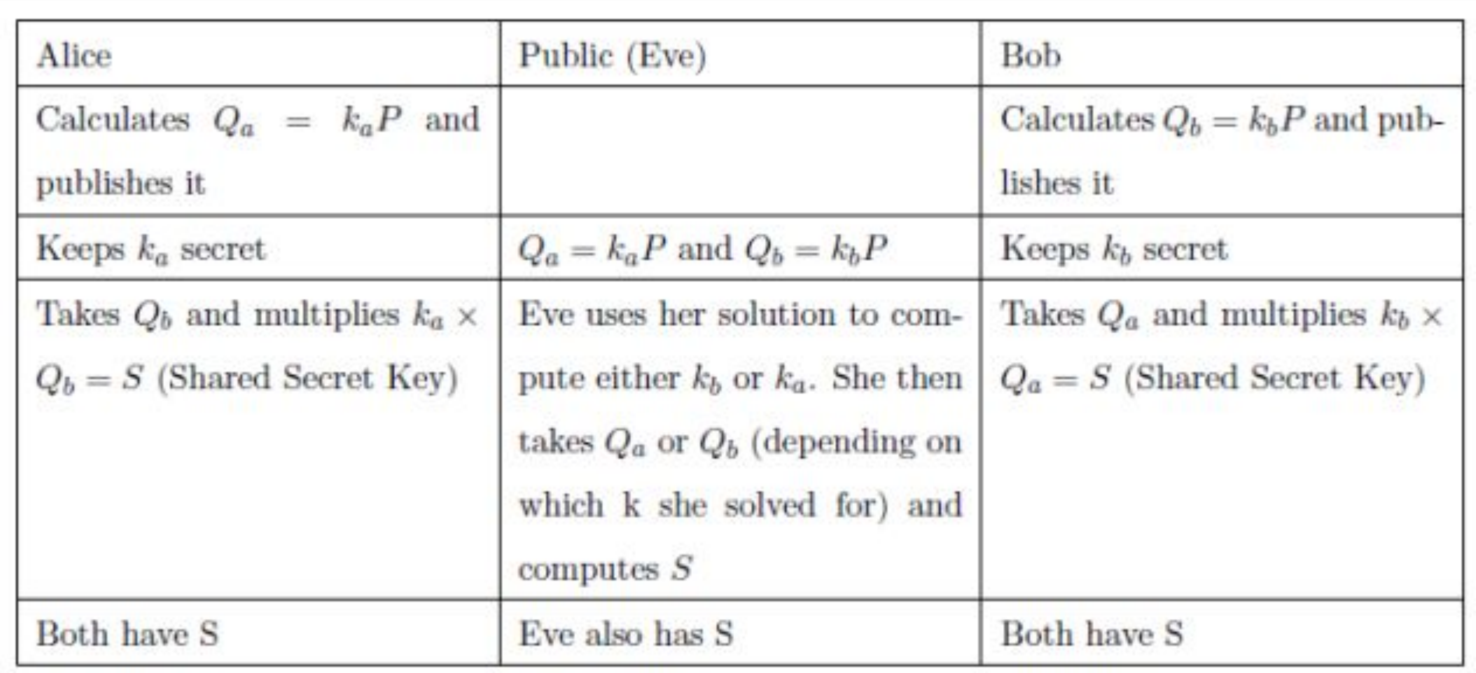
iii. Qa = kaP and Qb = kbP

Private Information:

i. ka and kb, where k is some large integer value

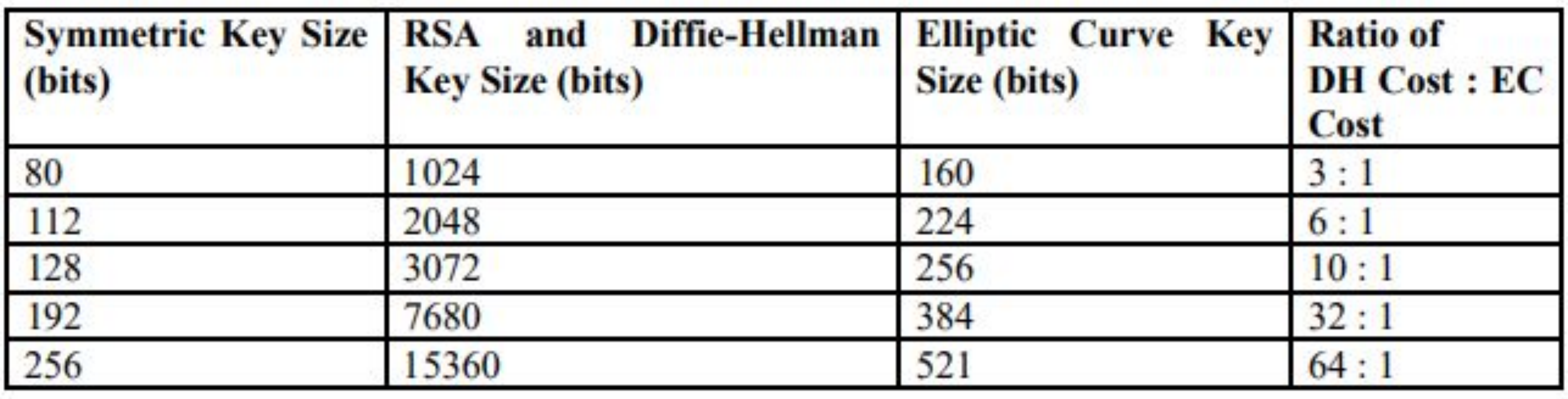
Elliptic Curve Diffie Hellman (ECDH)

Key Generation:



Alice	Public (Eve)	Bob
Calculates $Q_a = k_a P$ and publishes it		Calculates $Q_b = k_b P$ and publishes it
Keeps k_a secret	$Q_a = k_a P$ and $Q_b = k_b P$	Keeps k_b secret
Takes Q_b and multiplies $k_a \times Q_b = S$ (Shared Secret Key)	Eve uses her solution to compute either k_b or k_a. She then takes Q_a or Q_b (depending on which k she solved for) and computes S	Takes Q_a and multiplies $k_b \times Q_a = S$ (Shared Secret Key)
Both have S	Eve also has S	Both have S

Results



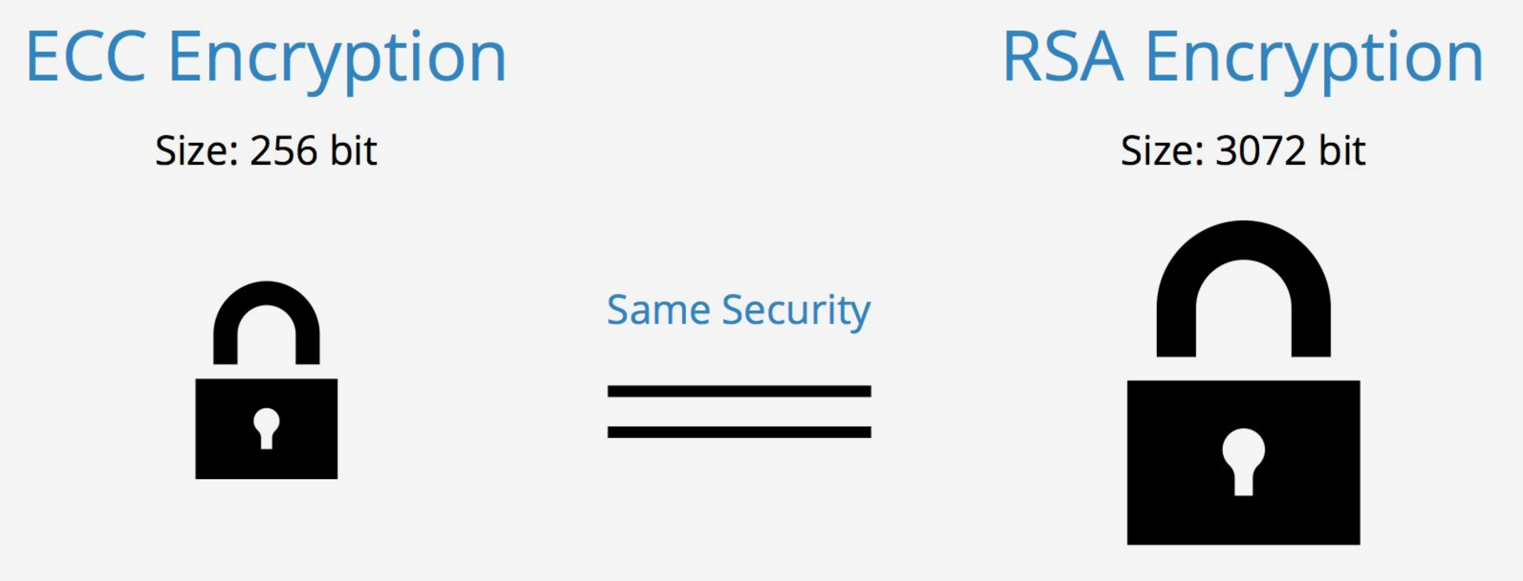
Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)	Ratio of DH Cost : EC Cost
80	1024	160	3 : 1
112	2048	224	6 : 1
128	3072	256	10 : 1
192	7680	384	32 : 1
256	15360	521	64 : 1

However, Elliptic Curve Algorithms are prone to Side Channel attacks

https://m.tau.ac.il/~tromer/mobilesc/

Conclusion

Elliptic Curve Techniques can be used to generate minimal key for installing blockchain on mobile device.



Thank You