RSA, ECC

Cryptography: course for master's degree in EDGE COMPUTING

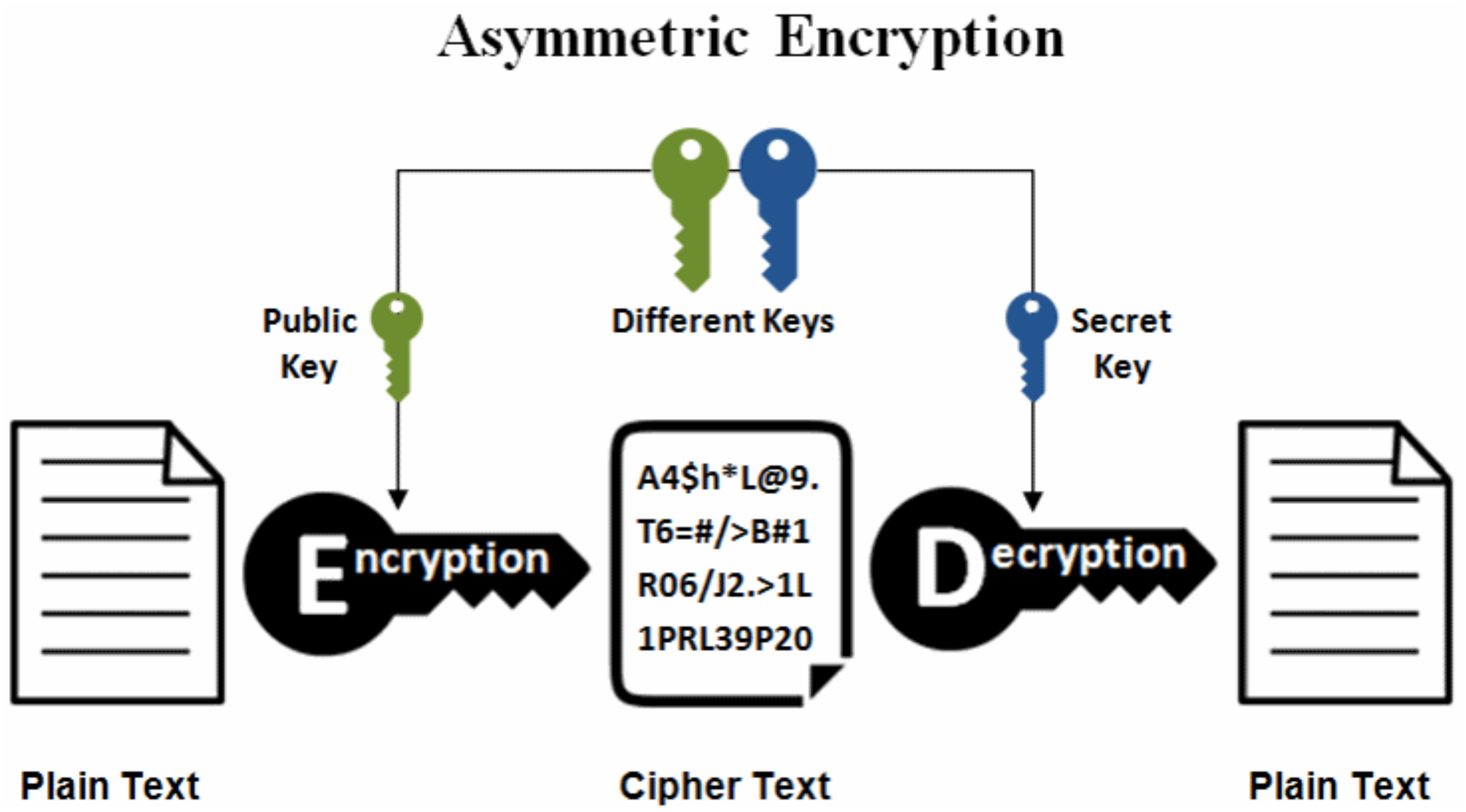
Michał Melosik, PhD

Lecture outline

1. Public and private key
2. RSA and key exchange protocols
3. RSAvisual as a education tool
4. ECC
5. ECCvisual as a education tool
6. Discussion

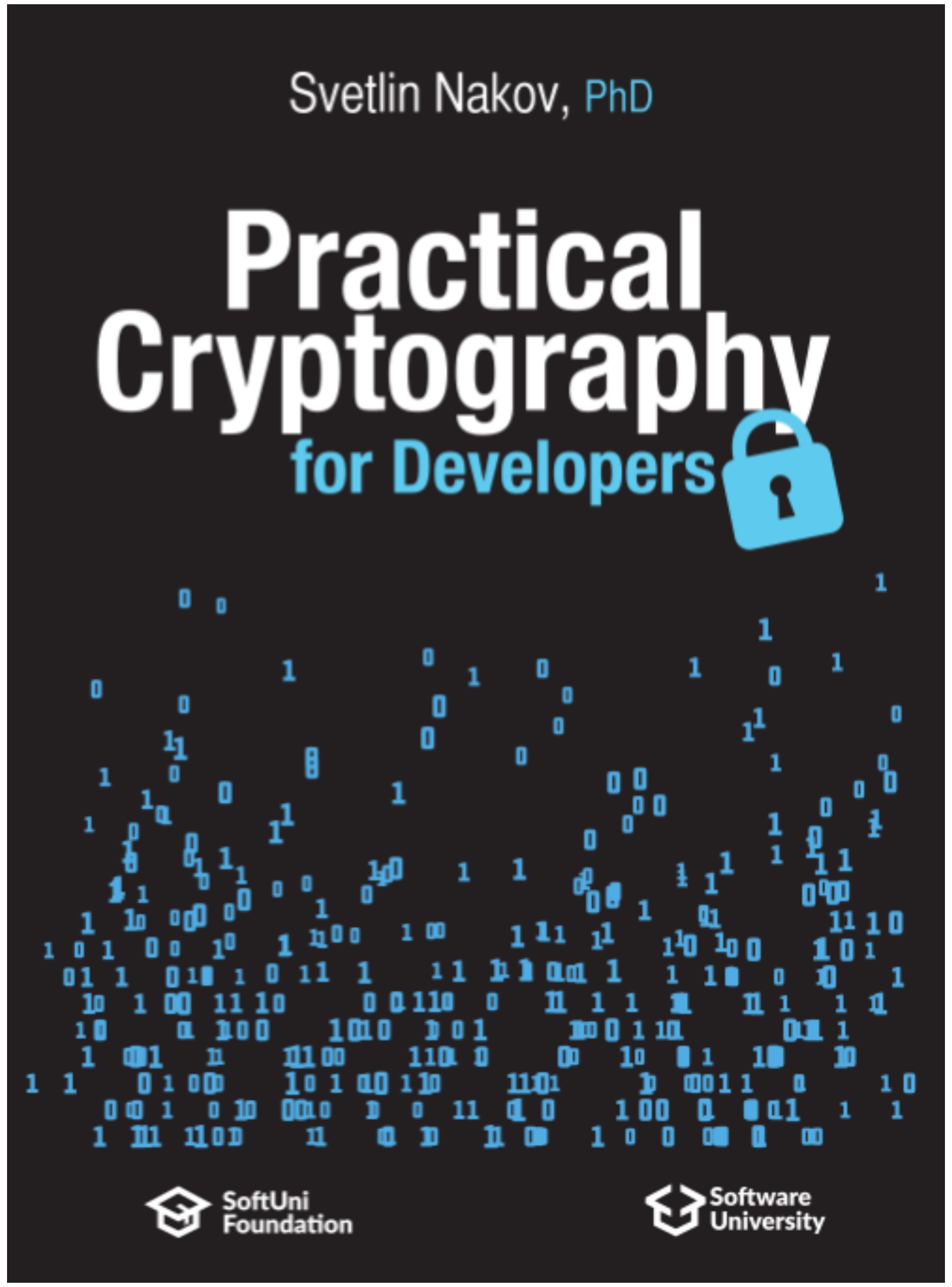
Asymmetric cryptography

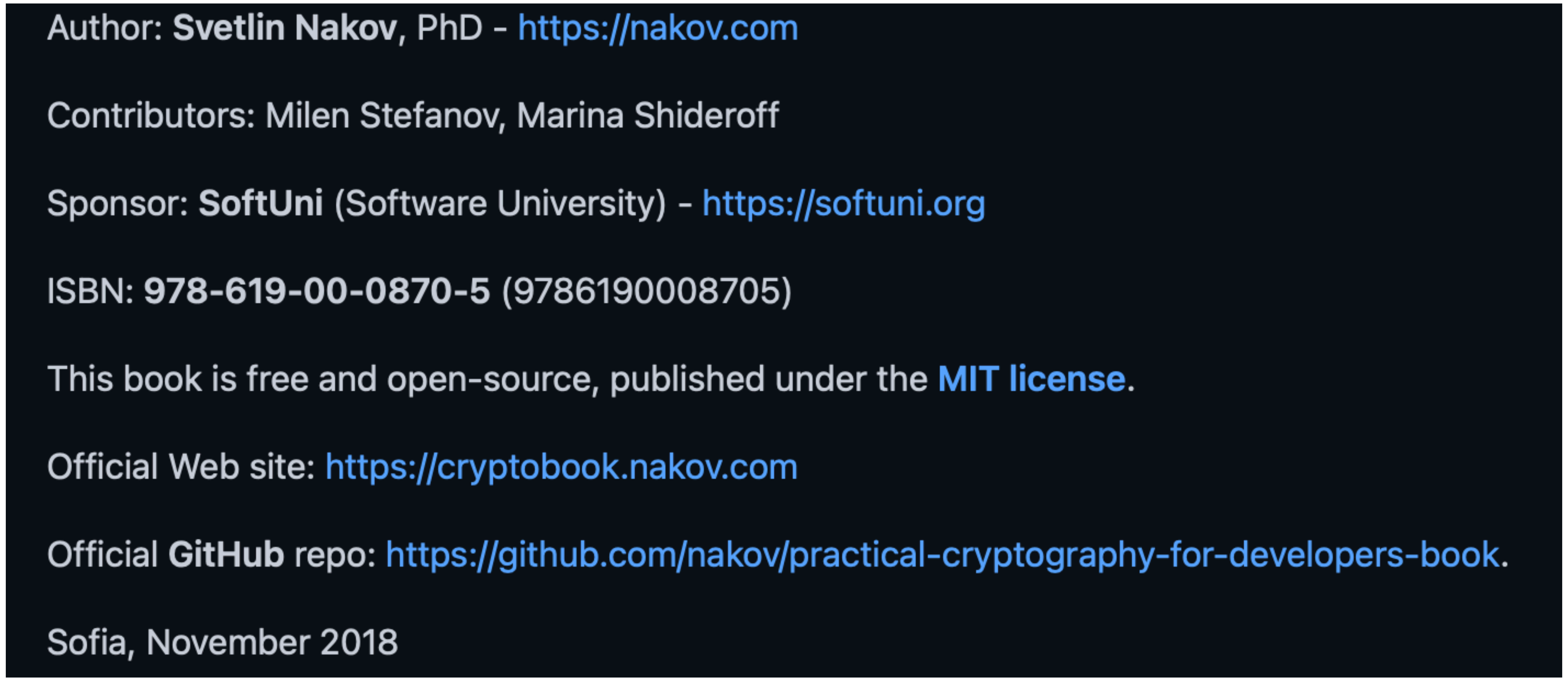
Idea



Source: https://github.com/nakov/Practical-Cryptography-for-Developers-Book/blob/master/asymmetric-key-ciphers/ecc-encryption-decryption.md

Asymmetric cryptography





Author: **Svetlin Nakov**, PhD - https://nakov.com

Contributors: Milen Stefanov, Marina Shideroff

Sponsor: **SoftUni** (Software University) - https://softuni.org

ISBN: **978-619-00-0870-5** (9786190008705)

This book is free and open-source, published under the **MIT license**.

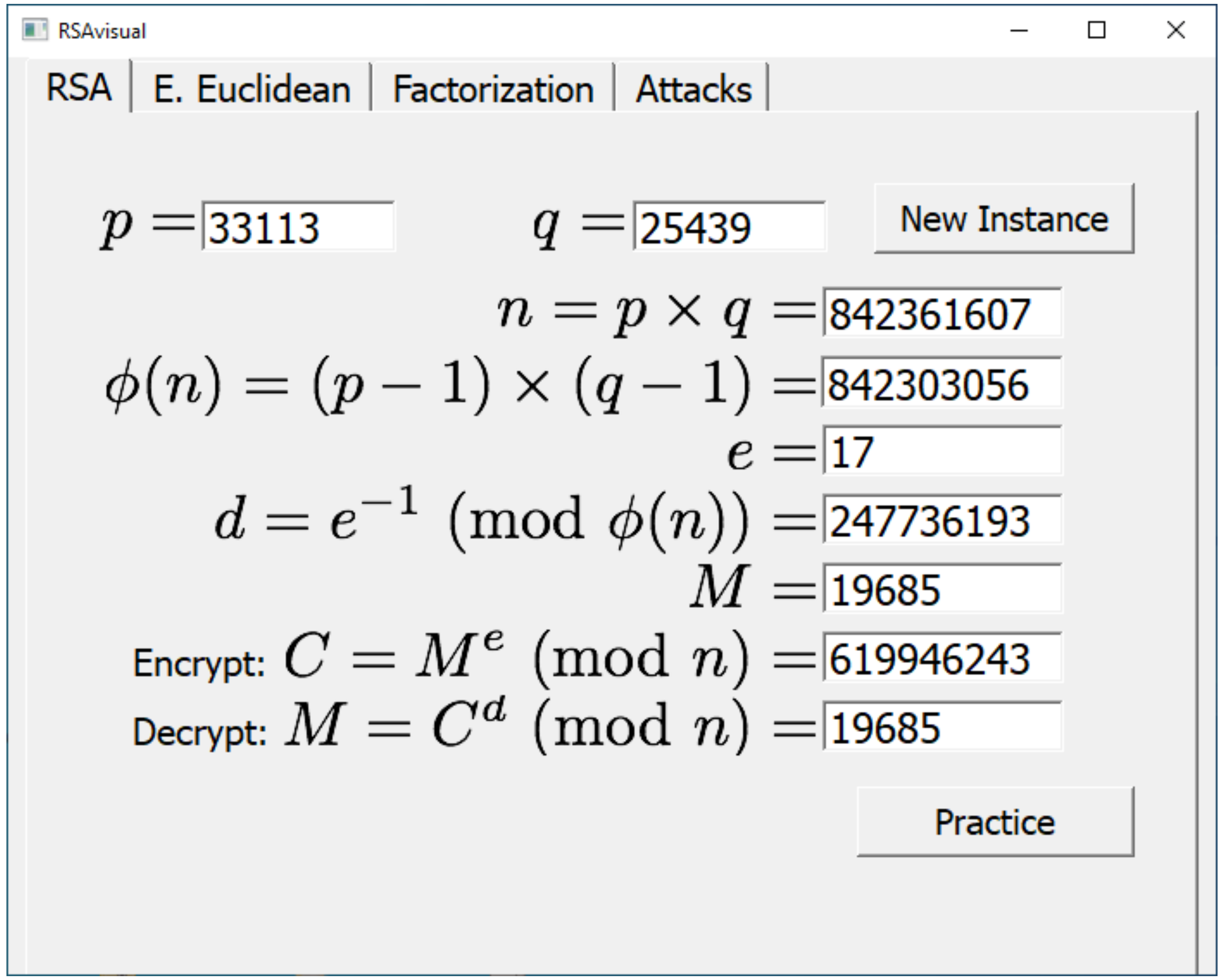
Official Web site: https://cryptobook.nakov.com

Official **GitHub** repo: https://github.com/nakov/practical-cryptography-for-developers-book.

Sofia, November 2018

RSA

Background



$p =$ 33113 $q =$ 25439

$n = p \times q =$ 842361607

$\phi(n) = (p-1) \times (q-1) =$ 842303056

$e =$ 17

$d = e^{-1} \pmod{\phi(n)} =$ 247736193

$M =$ 19685

Encrypt: $C = M^e \pmod{n} =$ 619946243

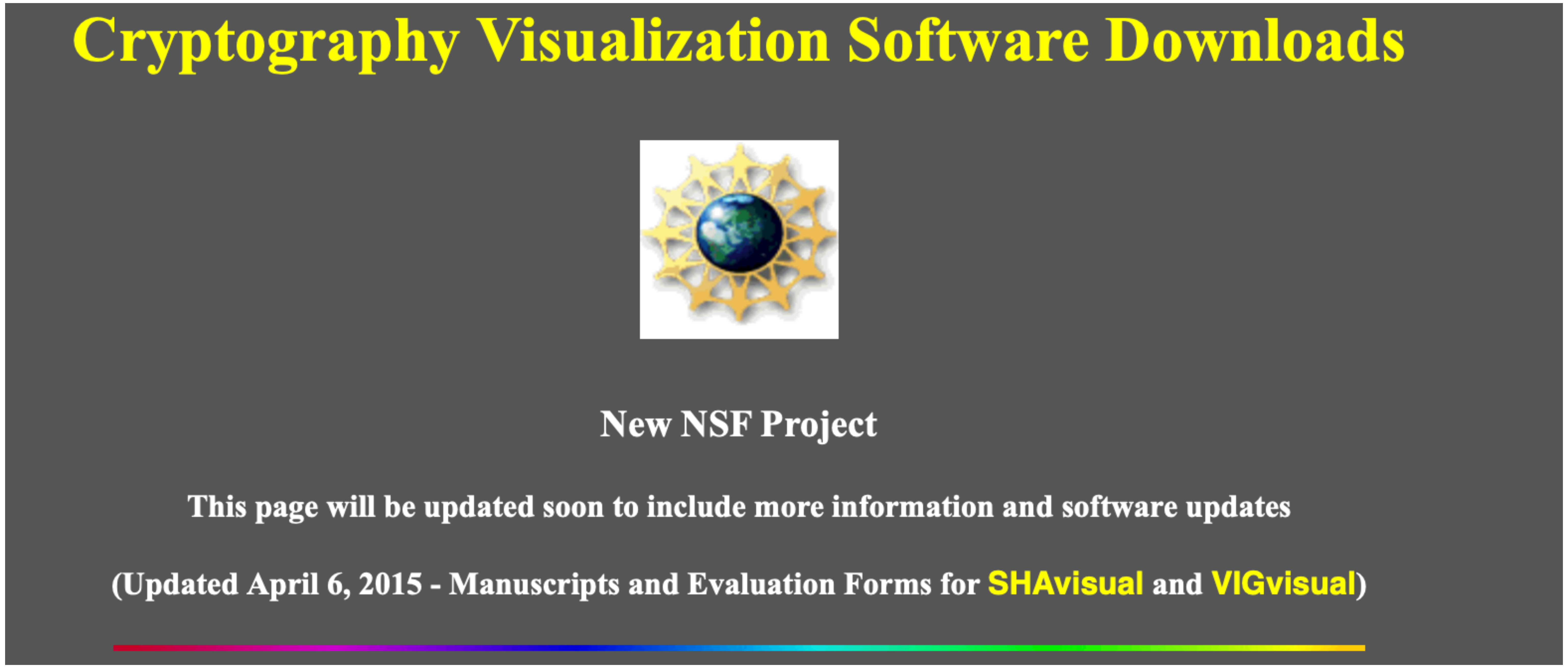
Decrypt: $M = C^d \pmod{n} =$ 19685

External video for teaching purposes - analysis during the lecture:

1. https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/intro-to-rsa-encryption
2. https://www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/diffie-hellman-key-exchange-part-2

RSAVisual

How to understand it?

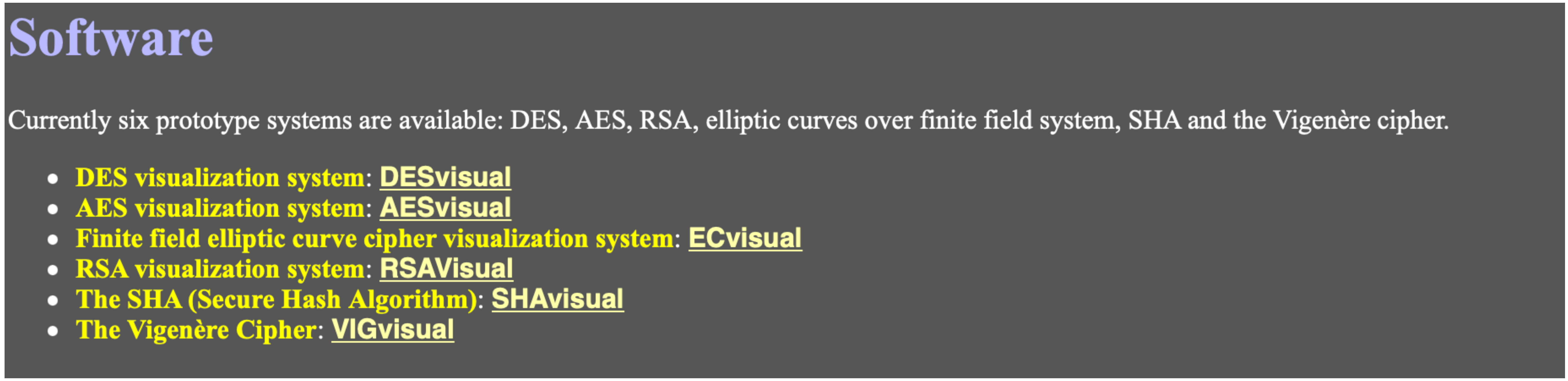


Cryptography Visualization Software Downloads

New NSF Project

This page will be updated soon to include more information and software updates

(Updated April 6, 2015 - Manuscripts and Evaluation Forms for SHAvisual and VIGvisual)



Software

Currently six prototype systems are available: DES, AES, RSA, elliptic curves over finite field system, SHA and the Vigenère cipher.

- DES visualization system: DESvisual
- AES visualization system: AESvisual
- Finite field elliptic curve cipher visualization system: ECvisual
- RSA visualization system: RSAVisual
- The SHA (Secure Hash Algorithm): SHAvisual
- The Vigenère Cipher: VIGvisual

Source: https://pages.mtu.edu/~shene/NSF-4/

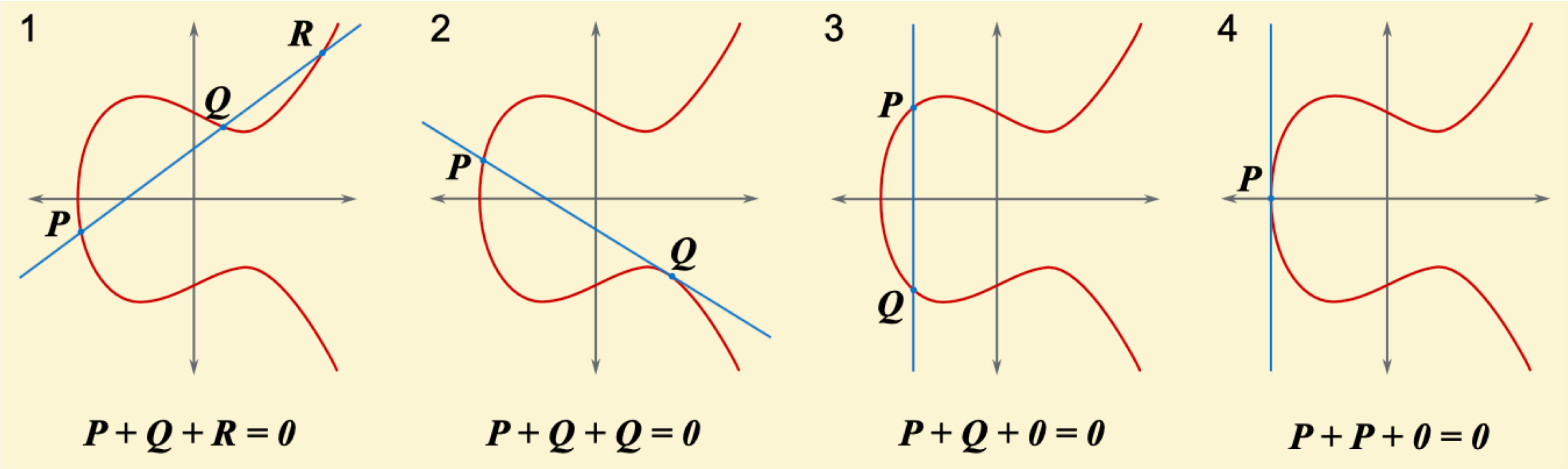
ECC

ECC - Elliptic-Curve Cryptography and is the newest encryption method. It is used with the ECDSA digital signature algorithm, which is characterized by high security, increased efficiency and shorter key lengths.

Like any public key cryptography, ECC is based on mathematical functions that are easy to compute in one direction, but very difficult to reverse. In the case of ECC, the difficulty lies in the infeasibility of calculating the discrete logarithm of a random element of an elliptic curve with respect to a commonly known base point, or in the "discrete logarithm problem of an elliptic curve”

ECC

Background



Source: https://cryptohack.org/courses/elliptic/bg/

Some external example: https://www.allaboutcircuits.com/technical-articles/elliptic-curve-cryptography-in-embedded-systems/

ECC

How to understand it?

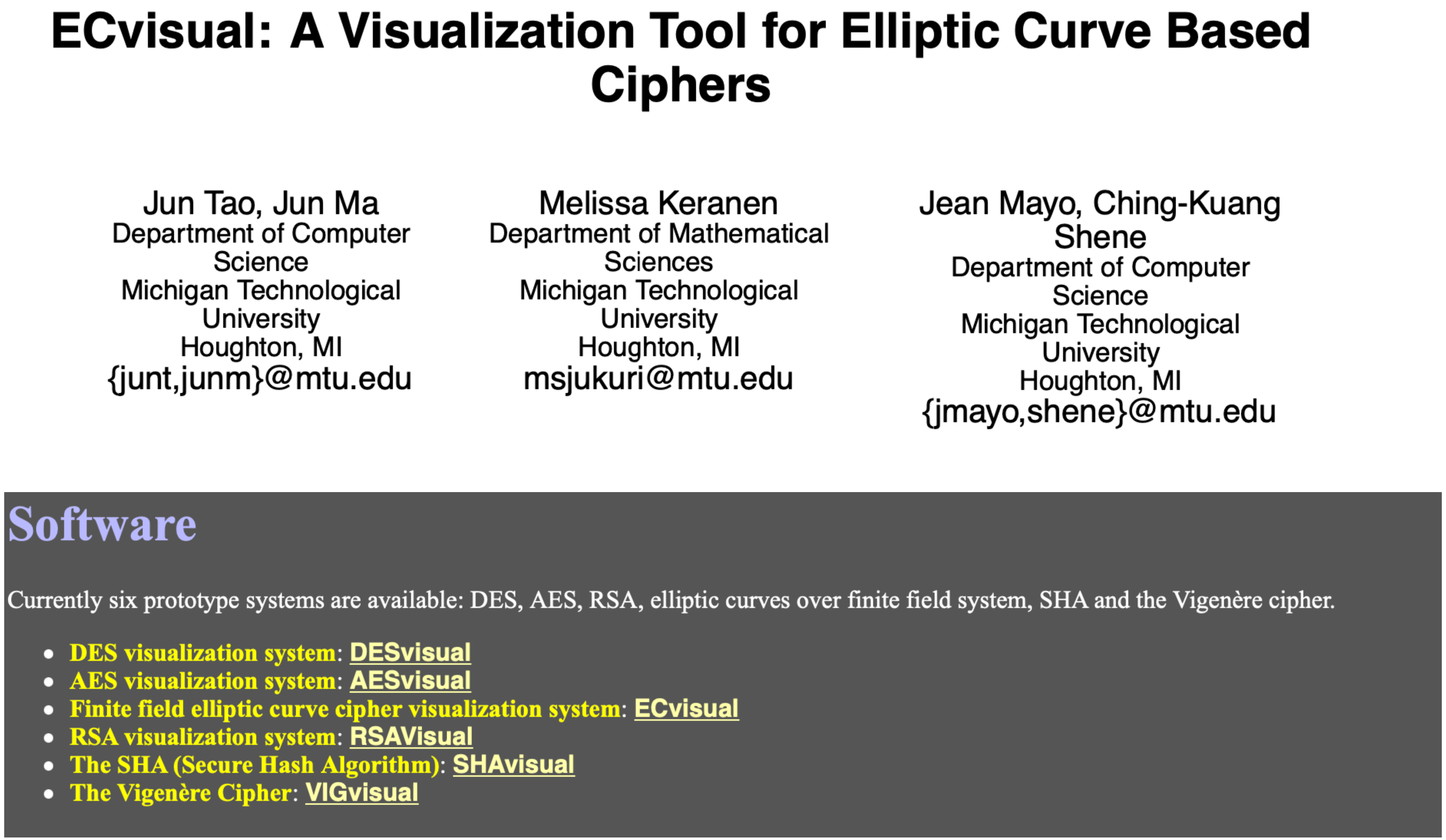
Cryptography Visualization Software Downloads

New NSF Project

This page will be updated soon to include more information and software updates

(Updated April 6, 2015 - Manuscripts and Evaluation Forms for SHAvisual and VIGvisual)

Source: https://pages.mtu.edu/~shene/NSF-4/



ECvisual: A Visualization Tool for Elliptic Curve Based Ciphers

Jun Tao, Jun Ma
Department of Computer Science
Michigan Technological University
Houghton, MI
{junt,junm}@mtu.edu

Melissa Keranen
Department of Mathematical Sciences
Michigan Technological University
Houghton, MI
msjukuri@mtu.edu

Jean Mayo, Ching-Kuang Shene
Department of Computer Science
Michigan Technological University
Houghton, MI
{jmayo,shene}@mtu.edu

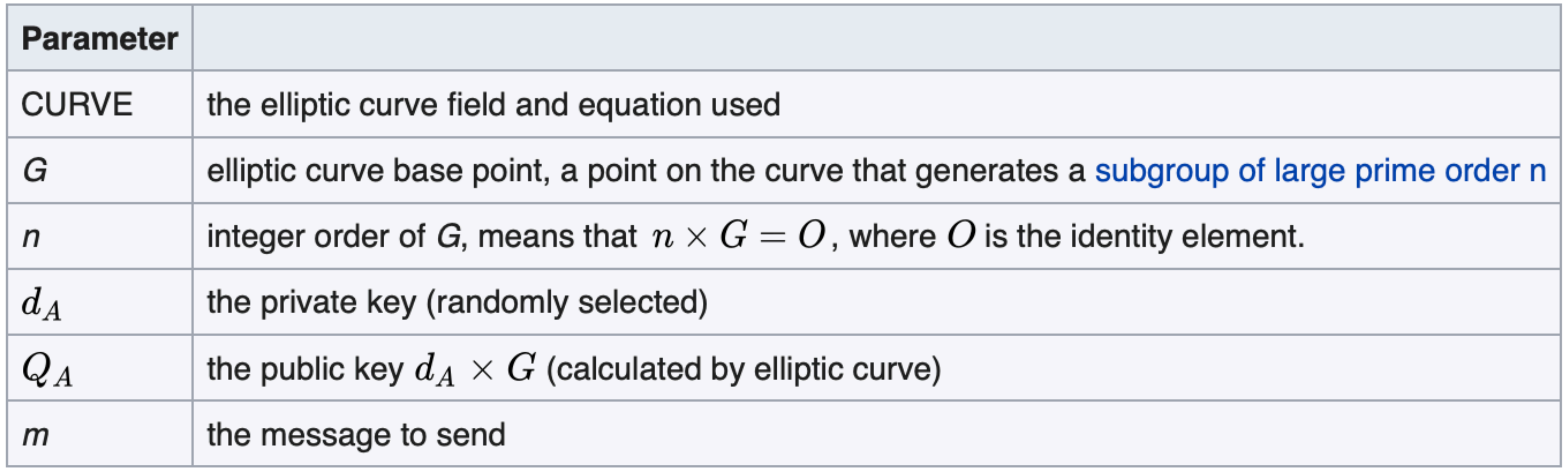
Software

Currently six prototype systems are available: DES, AES, RSA, elliptic curves over finite field system, SHA and the Vigenère cipher.

- **DES visualization system**: DESvisual
- **AES visualization system**: AESvisual
- **Finite field elliptic curve cipher visualization system**: ECvisual
- **RSA visualization system**: RSAVisual
- **The SHA (Secure Hash Algorithm)**: SHAvisual
- **The Vigenère Cipher**: VIGvisual

ECDSA

Elliptic Curve Digital Signature Algorithm (ECDSA) offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic-curve cryptography.



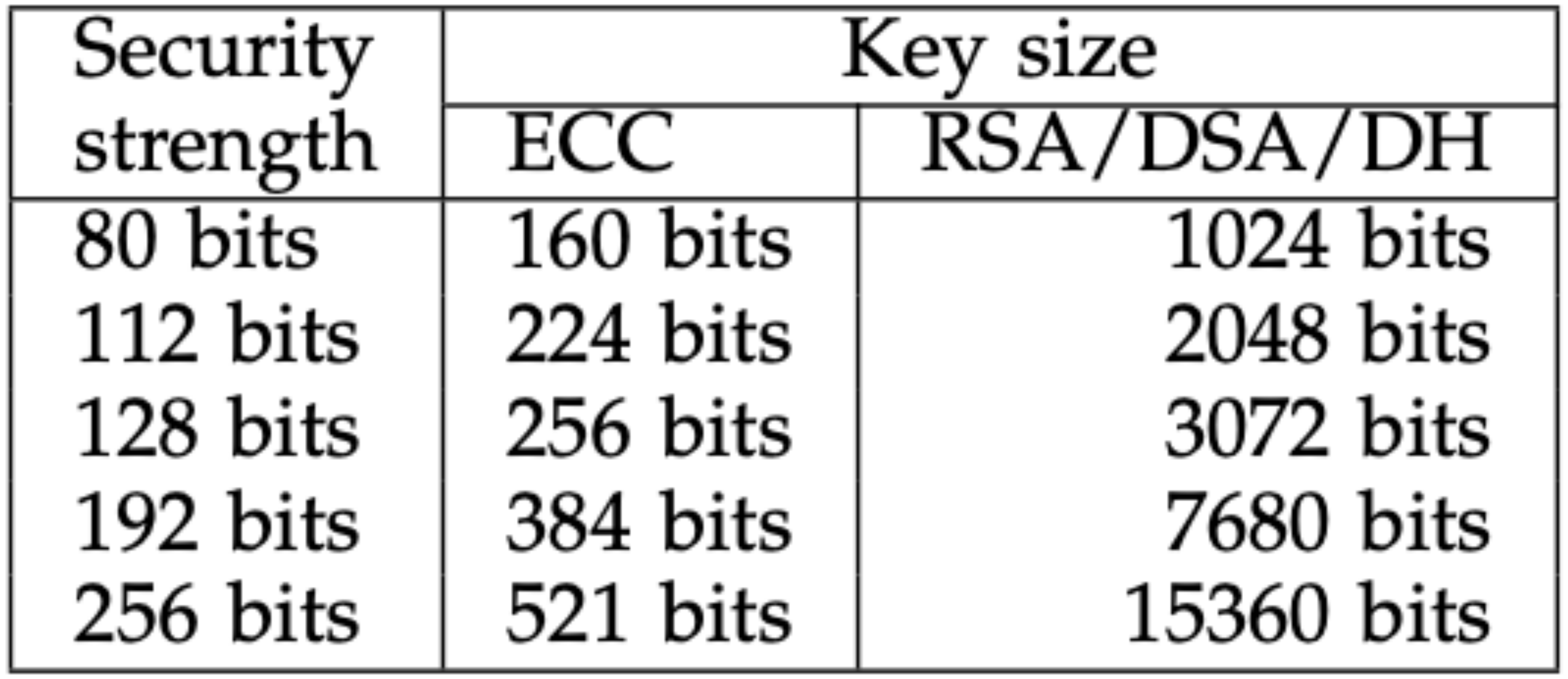
Parameter	
CURVE	the elliptic curve field and equation used
G	elliptic curve base point, a point on the curve that generates a subgroup of large prime order n
n	integer order of *G*, means that $n \times G = O$, where O is the identity element.
d_A	the private key (randomly selected)
Q_A	the public key $d_A \times G$ (calculated by elliptic curve)
m	the message to send

Some external example:

https://cryptobook.nakov.com/digital-signatures/ecdsa-sign-verify-messages

RSA vs ECC

Key length



Security strength	Key size	
	ECC	RSA/DSA/DH
80 bits	160 bits	1024 bits
112 bits	224 bits	2048 bits
128 bits	256 bits	3072 bits
192 bits	384 bits	7680 bits
256 bits	521 bits	15360 bits

Source:
Aitzhan, Nurzhan Zhumabekuly, and Davor Svetinovic. "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams." *IEEE Transactions on Dependable and Secure Computing* 15.5 (2016): 840-852.