2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

More Fun with Prime Numbers

Week 4

Homework

Tetsushi Ito

Department of Mathematics
Kyoto University

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

Problem 1

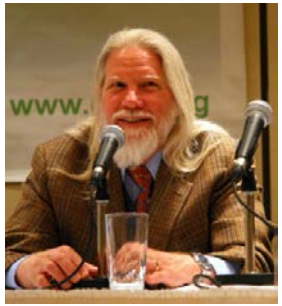
Choose the cryptosystem for which **exponentiation (mod P)** is used to encrypt the messages, and its security is based on the hardness of the **Discrete Logarithm Problem**.

(a) The Diffie-Hellman Key Exchange
(b) The RSA Cryptosystem
(c) The ElGamal Encryption System
(d) The Miller-Koblitz Elliptic Curve Cryptosystem

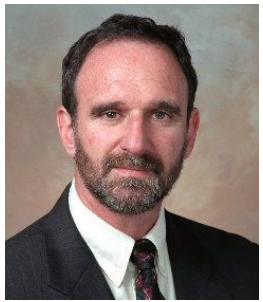
Problem 1

(a) Diffie-Hellman Key Exchange

- A method to share a secret key using **exponentiation (mod P)**.
- Diffie and Hellman could not find a method to encrypt messages.



Bailey Whitfield Diffie (1944-)



Martin Edward Hellman (1945-)

https://en.wikipedia.org/wiki/Whitfield_Diffie
https://en.wikipedia.org/wiki/Martin_Hellman

Problem 1

(b) The RSA Cryptosystem

- The first practical public key encryption system invented by Rivest, Shamir, Adleman.
- Exponentiation **(mod N=PQ)** is used.
- Security: **Integer Factorization Problems**

Ronald Linn Rivest (1947-)

Adi Shamir (1952-)

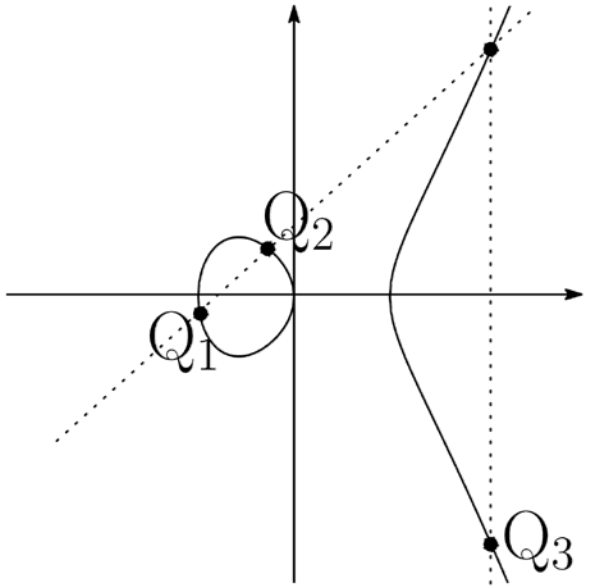
Leonard Adleman (1945-)

https://en.wikipedia.org/wiki/Ron_Rivest
https://en.wikipedia.org/wiki/Adi_Shamir
https://en.wikipedia.org/wiki/Leonard_Adleman

Problem 1

(d) The Miller-Koblitz Elliptic Curve Cryptosystem

- ECC is invented by Miller and Koblitz in 1985.
- ECC is being widely used.
- Security: **Elliptic Curve Discrete Logarithm Problem**



2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199

Problem 1

Answer (c) The ElGamal Encryption System

- It is invented by Elgamal in 1985 based on Diffie-Hellman's ideas.
- Exponentiation **(mod P)** is used.
- Security: **Discrete Logarithm Problem**

Taher Elgamal
(1955-)

https://en.wikipedia.org/wiki/Taher_Elgamal