INF 638
Cryptography & Cryptosystems

Class 1: Motivation & Definitions

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu

Cybersecurity

- INF 638: *Cryptography & Cryptosystems*
- INF 639: *Use of nanotechnologies*

Grading INF633B-CS599 Spring 2018

Assignment			Grade Weight %
Attendance (no miss: 100%)	miss 1 week:	75%	15%
	miss 2 weeks:	50%	
	miss 3 weeks:	25%	
	miss 4 weeks:	0%	
In class assignments	participate, very active:	100%	15%
	Do not participate:	0%	
Homework assignments	High quality work; >90%:	100%	15%
	Quality work; >70%:	75%	
	Poor quality; <70%	0-50%	
Research project #1:	Demonstrate understanding of the basic concepts		15%
Research project #2:	Demonstrate understanding of the advanced concepts		15%
Research project #3:	Demonstrate ability to implement and generalize		15%
Final report:	Ability to offer synthetic view		10%

INF 638: Cryptography & Cryptosystems

- 1- Motivation & Definitions
- 2- Elements of Number theory M
- 3- Early Cryptographic methods
- 4- Symmetrical Cryptography: DES
- 5- Symmetrical Cryptography: AES M
- 6- Quantum Cryptography: Key distribution
- 7- Elements of Asymmetrical Cryptography
- 8- Asymmetrical Cryptography: RSA M
- 9- ECC Key Distribution M
- 10- PKI & Digital Signatures
- 11- Hash Functions
- 12- Smartcards

Motivation & Definitions

- 1-1 Motivation for the course
- 1-2 Definitions in cryptography
- 1-3 Symmetrical cryptography
- 1-4 Asymmetrical cryptography
- 1-5 Stream ciphers and block ciphers

Cybersecurity at NAU

- **Start date:** August 2015 as part of the Electrical Engineering Department
- **Start up funds**: Dr. Cheng approved a fund of $800,000 in November 2015
- **ABOR:** Arizona board of Regent approved a $1,00,000 tri-university research program from May 2016 to Dec 2018:
  "Use of nanotechnologies for end-to-end cybersecurity solutions"
- **Graduate class INF633** "topics in cybersecurity – use of nanotechnology for cryptography". Start teaching fall 2016.
- **The cybersecurity lab opening** as part of the newly created school of Informatics, Computing, and Cyber Systems in August 2016.
  Equipment delivered from Dec 2016 to Oct 2017

Cybersecurity at NAU

- **The US Air Force** funded a $500,000 research program from April 2017 to Jan 2018: *"Benchmarking of ternary computing for information Insurance"*
- **Graduate class INF 633** "topic in cybersecurity" separated into two classes:
  - INF633/CS599: Elements of cryptography → **INF 638 (fall)**
  - INF633/EE599: Nanoelectronics for cybersecurity → **INF 639 (spring)**
- **BRIDG inc.** approved a $50,000 research program: *study CBRAM for cybersecurity*
- **National Science Fundation:** approval of a research program in Aug 2018: $750,000 over 3 years
- **Active publications:** 15 technical papers, 25 disclosures, 3 patent granted
- **5 industrial partners** signed NDA & licensing agreements

Why is it so difficult to block cyberattacks?

Learning from past breaches will not prevent future breaches

- As much as one million new malware born everyday
- "Worms" can be dormant years before activation

Most cybersecurity solutions fix past breaches, not new ones

- Assume that breaches are due to lack of training, or policy breaches
- Antivirus, firewall, machine learning are all based on past breaches

Quantum computers will challenge cryptography

- Modern cryptography based on mathematics is vulnerable to QC

Why nanomaterials?

Micro-electronic components are now using nanomaterials

1µm (10^{-6}m) geometry in the early 90's ➔ 10nm (10^{-6}m) now ➔ 1nm expected in 2027

1nm represents about 10 atomic layers of silicon

Each component is subject to manufacturing variations that make them:

Unique

Unclonable

It is possible to extract electronic "fingerprints" from the nanostructures

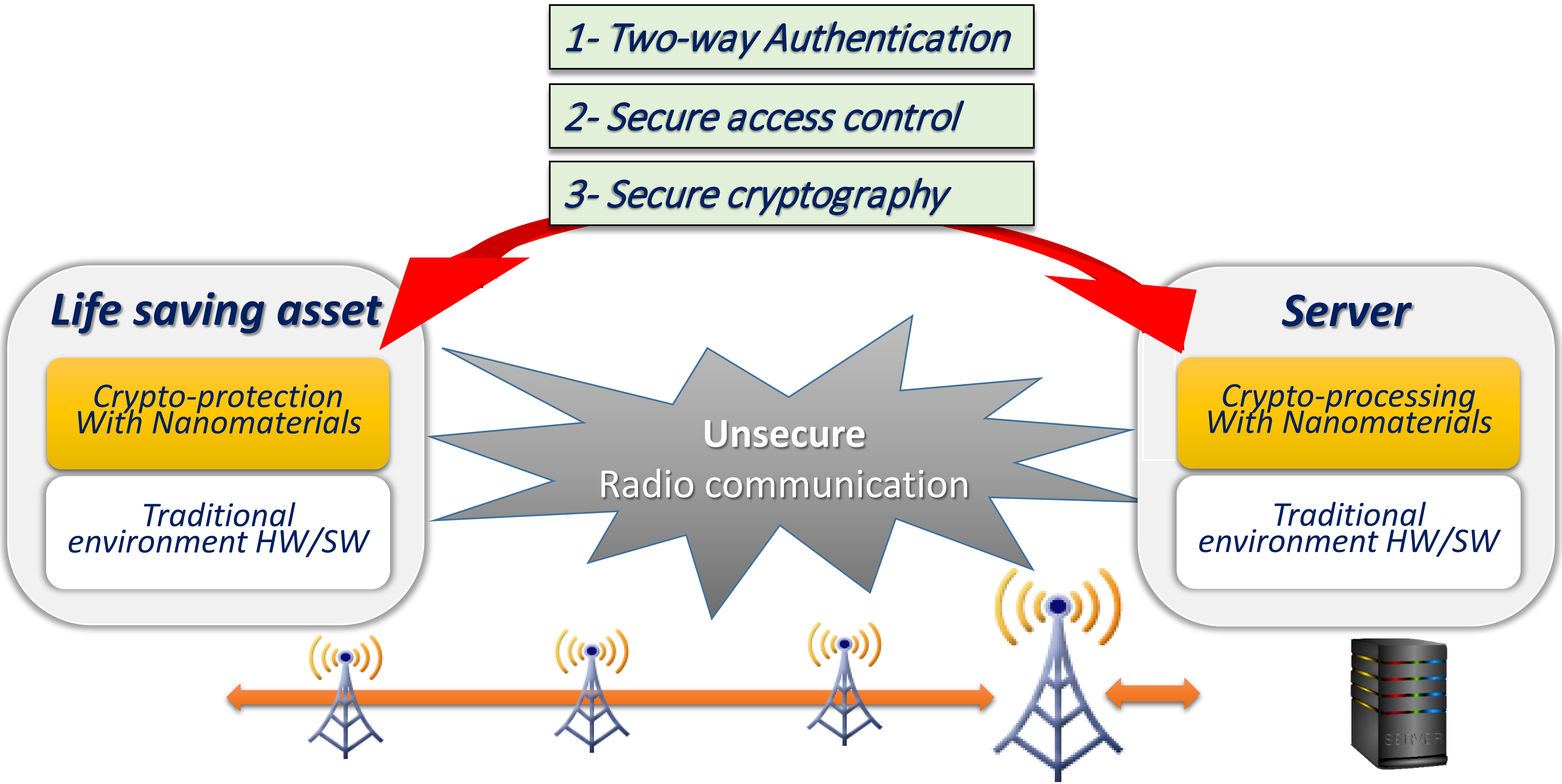
These "fingerprints" are called Physical Unclonable Functions (PUF)

It is also possible to develop a new class of cryptography based on PUFs

Several orders of magnitude more protective than traditional cryptography

Opportunity to be quantum computer resistant

Nanomaterials to protect life saving assets



Motivation & Definitions

- 1-1 Motivation of the course
- 1-2 Definitions in cryptography
- 1-3 Symmetrical cryptography
- 1-4 Asymmetrical cryptography
- 1-5 Stream ciphers and block ciphers

Some Definitions -1

- ***Cryptography***: From the Greek Kryptos (hidden, covered) & -graphy (writing). The art (or science) of protecting secret information and restrict communication to a selected audience
- ***Cryptographers***: The people who create methods to effectively hide secret information.
- ***Encryption***: Conversion of a plain message into a protected message also called a *cipher.*
- ***Decryption***: Conversion of a cypher into a plain message.
- ***Cryptoanalyst***: Individuals able to decrypt cyphers (also a *hacker*, or *code breakers)*.
- ***Cryptology***: the study of cryptography and cryptoanalysis.
- ***Identification***: unique Information describing a subject/object, can be used to identify it.
- ***Authentication***: Secret information confirming that the subject/object, is the right one.
- ***Access control***: Granting access based on secure authentication.

Some Definitions - 2

- ***Cryptographic key***: Secret stream of data (or combination) used in the encryption/decryption process.
- **Symmetrical cryptography:** Same key used to encrypt and decrypt messages.
- ***Asymmetrical cryptography***: The key to decrypt is different than the key to encrypt.
- ***Public key cryptography***: Asymmetrical cryptography using *public-private* keys.
- ***Cryptographic primitive***: Data stream involved in encryption such as *finger print, physically unclonable function, True Random number generator*.
- ***Biometry***: Generation of cryptographic primitive describing human unique characteristic (finger print, iris, heart beat, DNA, vein, brain signals ..)
- ***Physical Unclonable Functions***: Secret data stream (cryptographic primitive) based on unique characteristics of objects or micro-components.

Some Definitions -3

- ***Quantum cryptography***: When the laws of physics are used rather than mathematical algorithms. Existing methods restricted to key exchange.
- ***Post quantum computing cryptography:*** Cryptography capable to resist attacks conducted by quantum computers (or future quantum computers).
- ***Side channel analysis/attack***: Method to extract secret information while cryptography is performed
- ***Hash Function***: Function which take an input (plain text) and return it to a fixed size (smaller size) alphanumeric string, the *hash value*.
- ***Sumchecks***: Digest function that can flag the alteration of a message
- ***Message digest***: Hash value that is non keyed ➔ *message integrity code*,
  or keyed ➔ *message authentication code*.

Some acronyms – 1

- ***DES***: Data Encryption System – Symmetrical algorithm.
- ***AES***: Advanced Encryption System – Symmetrical algorithm.
- ***RSA:*** Rivest Shamir Adelman – Asymmetrical algorithm.
- ***ECC:*** Elliptic Curve Cryptography – Asymmetrical algorithm.
- ***DH:*** Diffie Hellman – Asymmetrical algorithm.
- ***Entropy:*** Level of chaos – Measure the level of randomness.
- ***PUF:*** Physically Unclonable Function – Cryptographic primitive.
- ***MIC:*** Message Integrity Code – Non-keyed message digest.
- ***MAC:*** Message Authentication Code – Keyed message digest.
- ***SHS/SHA:*** Secure Hash Standard/Secure Hash Algorithm.
- ***PKI:*** Public Key Infrastructure – Deployment of asymmetrical cryptography.

Some acronyms -2

- ***CA:*** Certificate Authority – manage digital certificate and key distribution.
- ***DSA:*** Digital Signature Algorithm.
- ***PRNG, TRNG, RNG:*** Pseudo, True Random Number Generator
- ***PGP:*** Pretty Good Privacy.
- ***S/MIME:*** Secure/Multipurpose Internet Mail Extension.
- ***SSL/TLS:*** Secure Socket Layer/Transport Layer Security.
- ***Ipsec/VPN:*** Internet Protocol Security/Virtual Private Network.
- ***SA/IKE:*** Security Association/Internet Key Exchange.
- ***DPA/SPA:*** Differential Power Analysis/Single Power Analysis.
- ***EMI:*** Electromagnetic interference

Motivation & Definitions

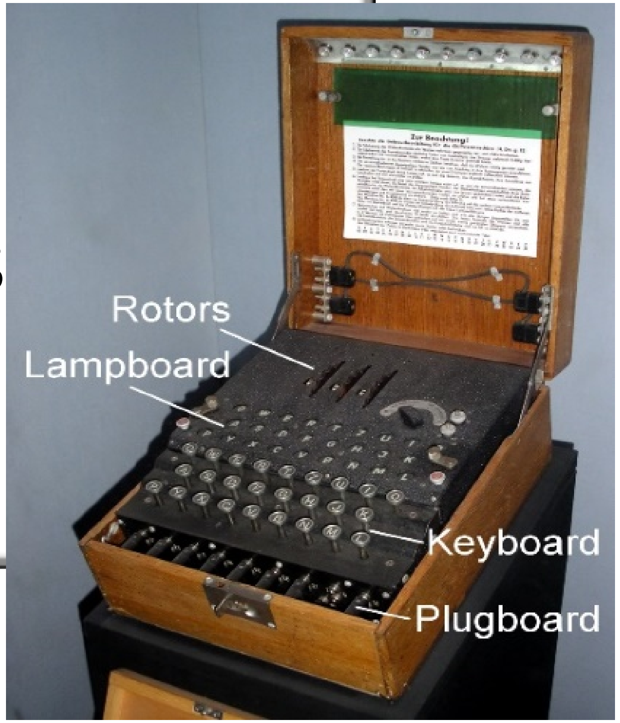
- 1-1 Motivation of the course
- 1-2 Definitions in cryptography
- 1-3 Symmetrical cryptography
- 1-4 Asymmetrical cryptography
- 1-5 Stream ciphers and block ciphers

Symmetrical Cryptography

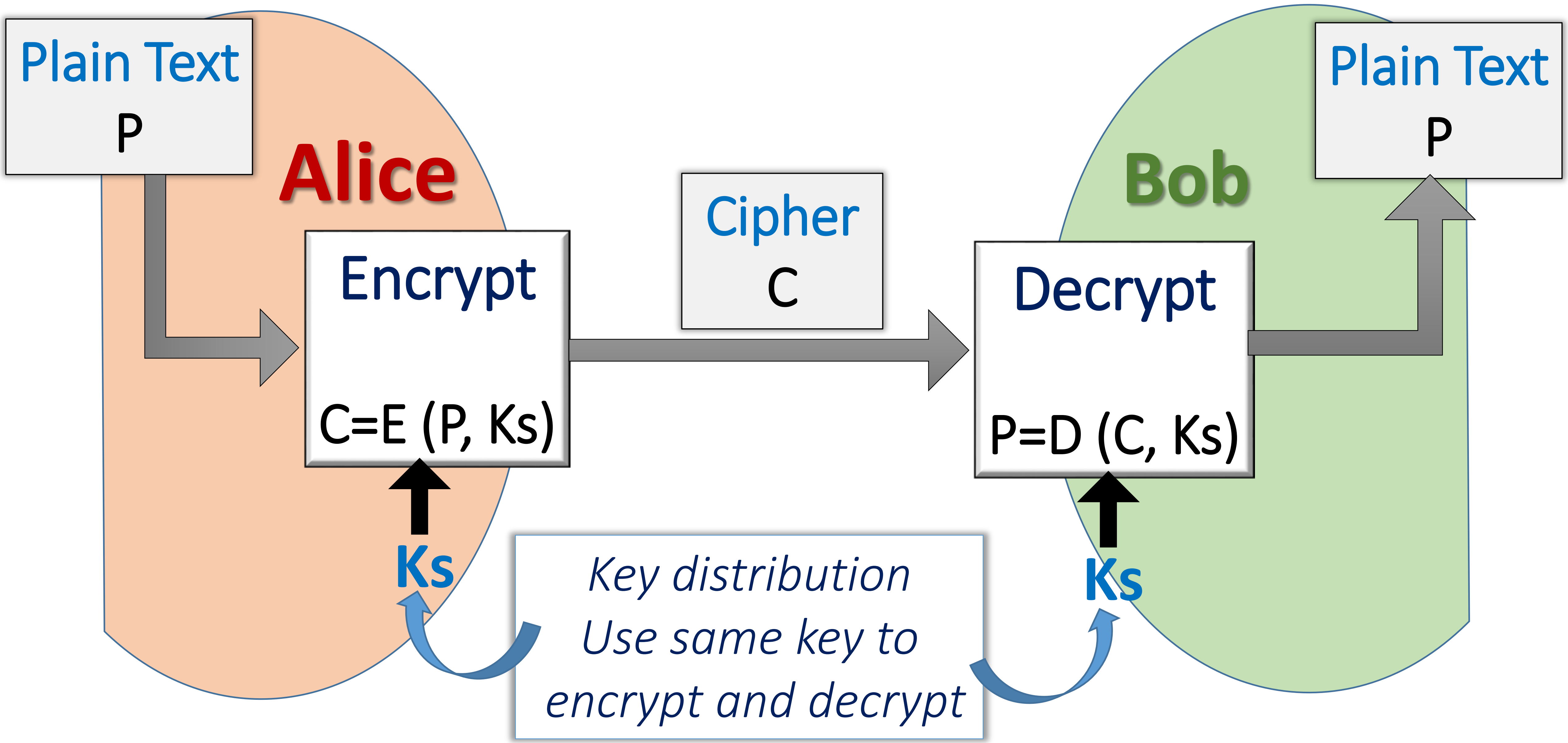
- Same key to encrypt and to decrypt
- Symmetrical Cryptography exist since the Romans
- Encryption and decryption methods is fast and effective
- Encryption/decryption methods can be secret, **or open**
- Does not really handle well multiple users

  (each communication need a private key)
- Limitation highlighted by famous code breakers

  (Alan Turing and the enigma)
- Still very important technology: DES, AES,…….



Symmetrical Cryptography



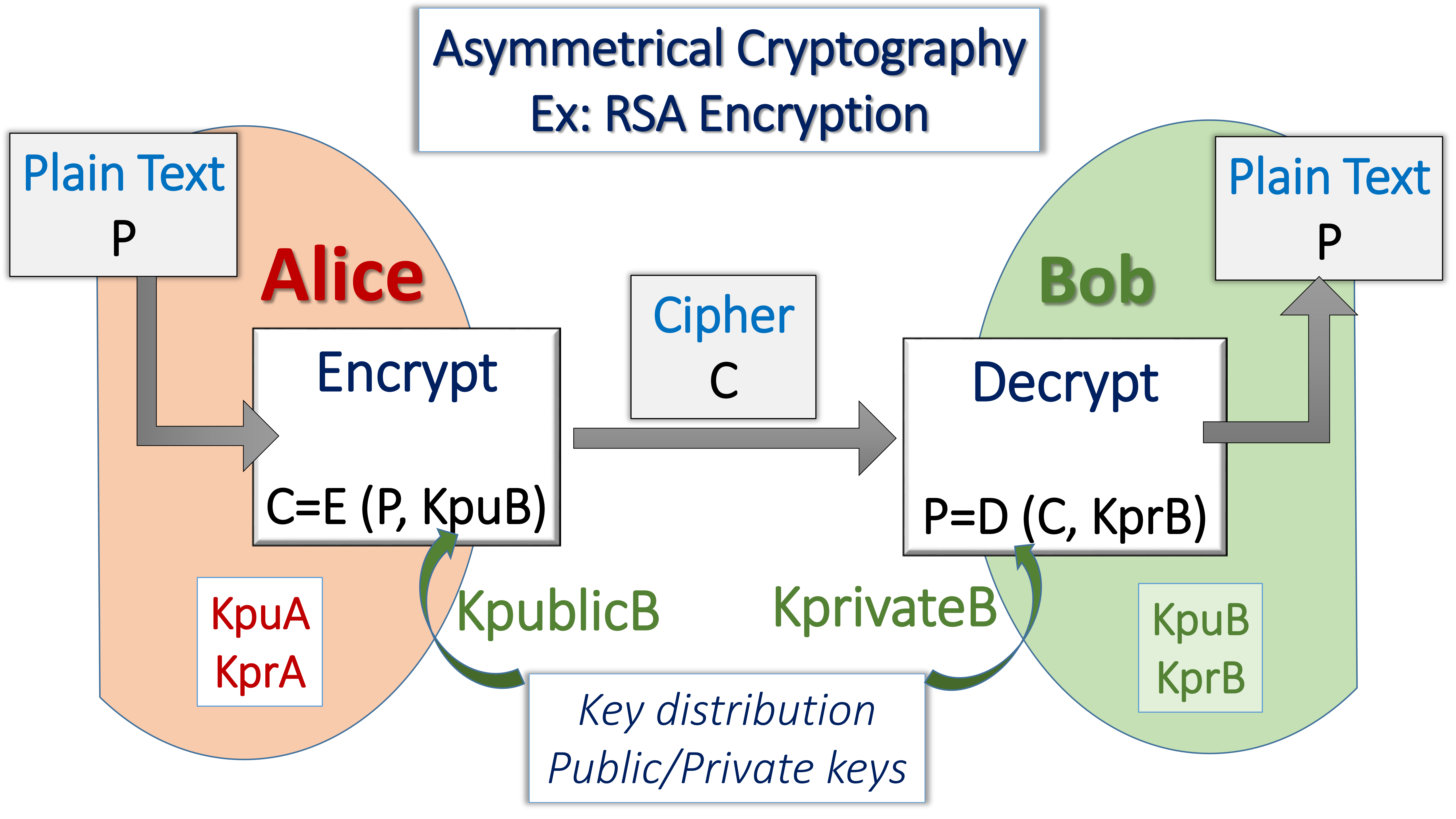
Motivation & Definitions

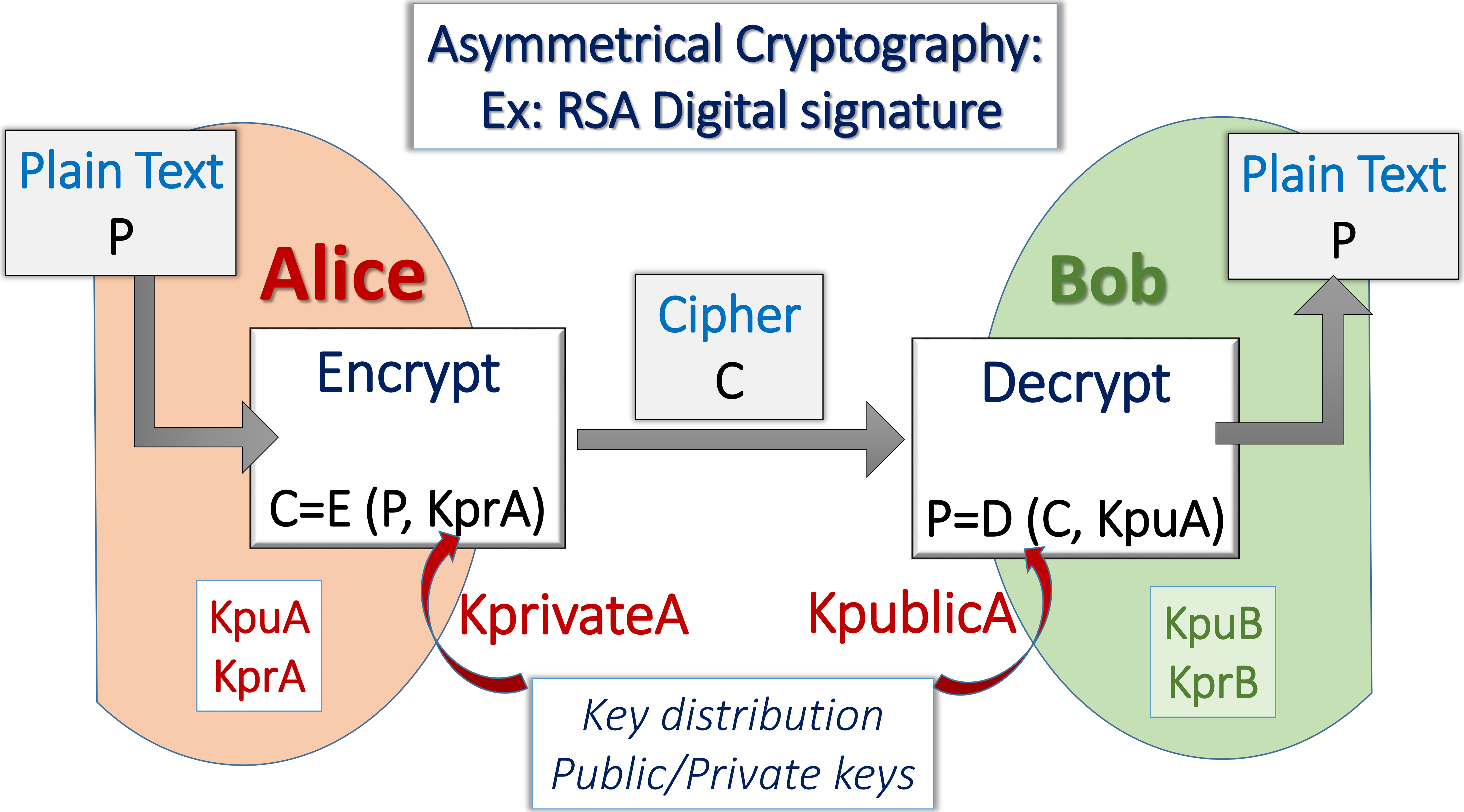
- 1- Motivation
- 2- Definitions
- 3- Symmetrical cryptography
- 4- Asymmetrical cryptography
- 5- Other ciphers

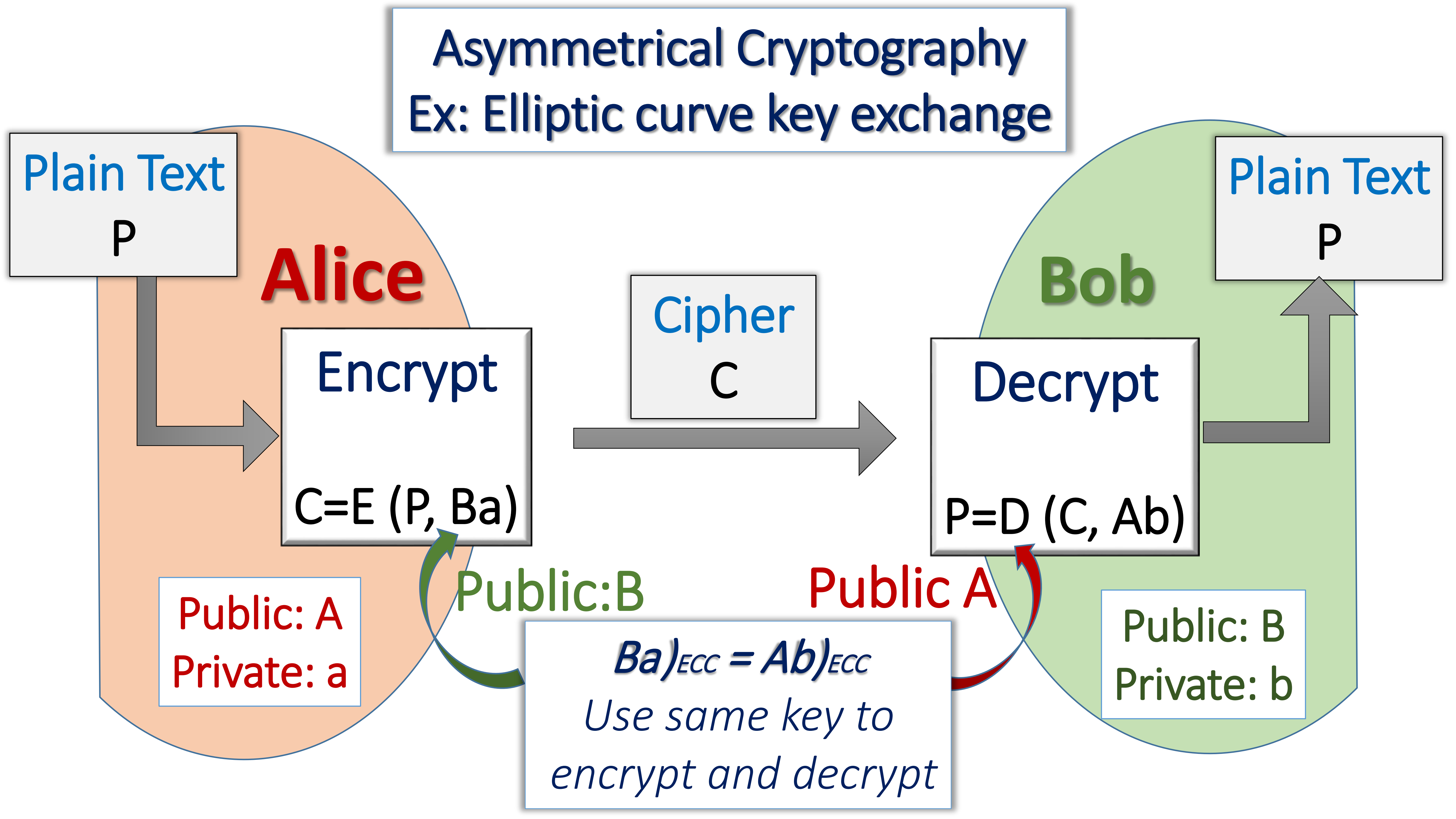
Asymmetrical Cryptography

- Different keys to encrypt and to decrypt
- Asymmetrical Cryptography invented the mid 80's
- Key exchange is very complex
- Encryption and decryption methods are complicated
- Encryption/decryption methods are totally **open**
- Perfect to handle multiple users

  (web, finance, telecommunication,....)
- Questionable with quantum cryptography
- Most important schemes: RSA, and ECC.


Asymmetrical Cryptography
Ex: RSA Encryption
Plain Text
P
Alice
Encrypt
C=E (P, KpuB)
Cipher
C
Decrypt
P=D (C, KprB)
Bob
Plain Text
P
KpuA
KprA
KpublicB
KprivateB
KpuB
KprB
Key distribution
Public/Private keys


Asymmetrical Cryptography:
Ex: RSA Digital signature
Plain Text
P
Alice
Encrypt
C=E (P, KprA)
KpuA
KprA
Cipher
C
KprivateA
KpublicA
Key distribution
Public/Private keys
Bob
Plain Text
P
Decrypt
P=D (C, KpuA)
KpuB
KprB


Asymmetrical Cryptography
Ex: Elliptic curve key exchange
Plain Text
P
Alice
Encrypt
C=E (P, Ba)
Cipher
C
Bob
Plain Text
P
Decrypt
P=D (C, Ab)
Public: A
Private: a
Public:B
Public A
Ba)ECC = Ab)ECC
Use same key to
encrypt and decrypt
Public: B
Private: b

Motivation & Definitions

- 1-1 Motivation of the course
- 1-2 Definitions in cryptography
- 1-3 Symmetrical cryptography
- 1-4 Asymmetrical cryptography
- 1-5 Stream ciphers and block ciphers

Stream cipher: continuous encryption

- All elements of the plain text encrypted with the same algorithm:

$$\boldsymbol{P} = \{\boldsymbol{P_1} \,; \boldsymbol{P_2} \,; \dots ; \boldsymbol{P_i} \,; \dots ; \boldsymbol{P_k} \,; \dots.\}$$

$$\boldsymbol{C_i} = \mathrm{E}(\,\boldsymbol{P_i}, \mathrm{Ks});$$

- Data stream “P” is converted in a sequential way to a cipher “C”
- Caesar cipher, and one time pad are examples of stream cipher
- One time pad: the key is as long as the plain text

Stream cipher: continuous encryption

Stream - plain

$\{P_1 \; ; P_2 \; ; \ldots ; P_j \; ; \ldots ; P_k \; ; \ldots.\}$

Stream - cipher

$\{C_1 \; ; C_2 \; ; \ldots ; C_j \; ; \ldots ; C_k \; ; \ldots.\}$

Plain Text

P

Encrypt

C=E (P, Ks)

C : stream cipher

E: stream cipher encryption

Ks : symmetrical key

Ks

Cipher

C

Block cipher

- The encryption is done block by block, not bit by bit
- No direct link between one single entry bit to one single output bit
- The plain text P is grouped into blocks having the same length "*k*"
- The encryption key is also a data stream of length *n*:

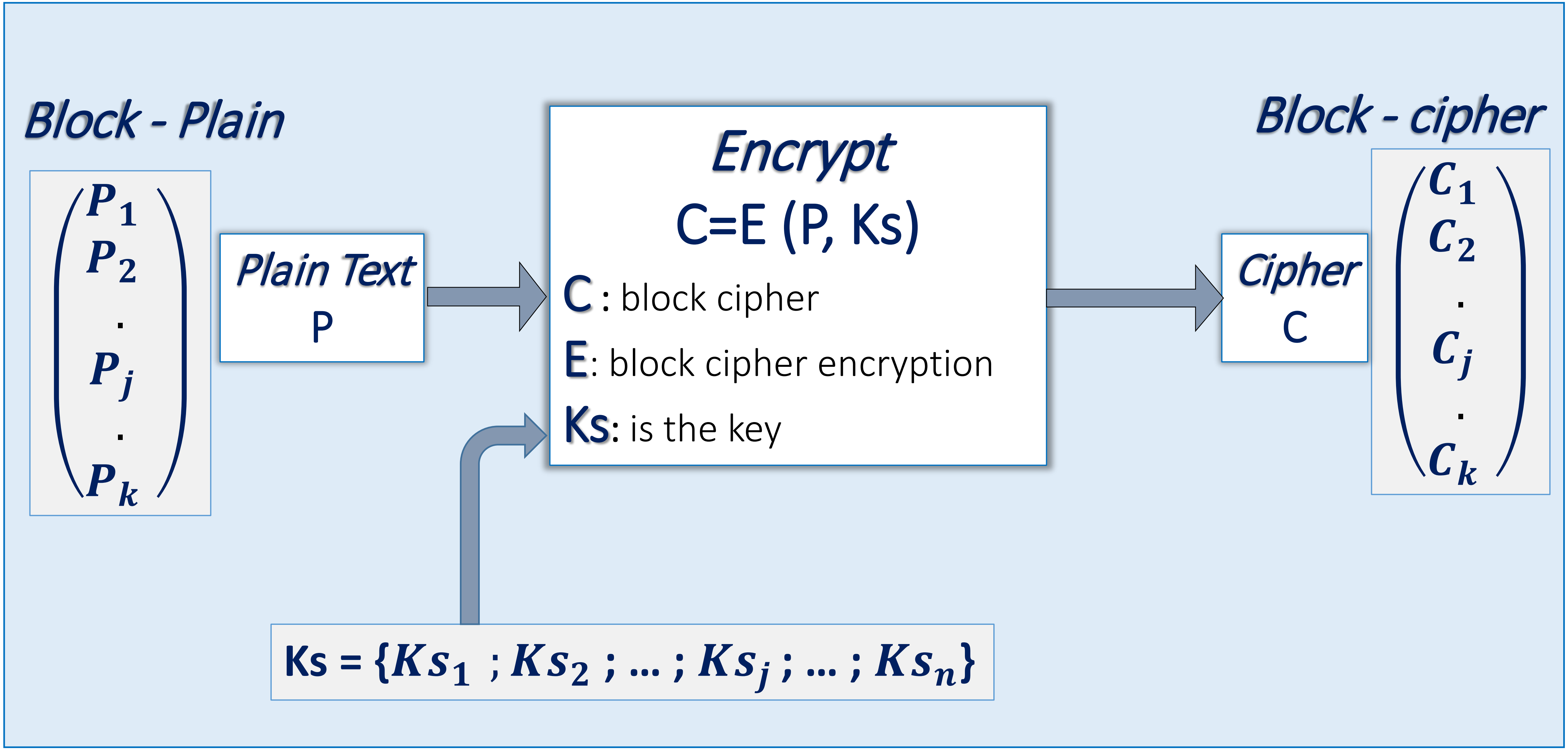
$$\boldsymbol{Ks} = \{\boldsymbol{Ks_1} ; \boldsymbol{Ks_2} ; \dots ; \boldsymbol{Ks_j} ; \dots ; \boldsymbol{Ks_n}\}$$

- The subgroups of *k* bits, or blocks are encrypted together:

$$\{\boldsymbol{C_{i1}} ; \boldsymbol{C_{i2}} ; \dots ; \boldsymbol{C_{ij}} ; \dots ; \boldsymbol{C_{ik}}\} = \mathrm{E}\,(\{\boldsymbol{P_{i1}} ; \boldsymbol{P_{i2}} ; \dots ; \boldsymbol{P_{ij}} ; \dots ; \boldsymbol{P_{ik}}\}, \mathrm{Ks})$$

- Three cases: *n=k* ; *n>k* ; *or n<k*
- Can be symmetrical or asymmetrical
- Examples of block ciphers includes DES, AES, and RSA.

Block cipher



Block cipher

k elements

Plain P: $p_{11};\dots;p_{1j};\dots;p_{1k};\dots;p_{i1};\dots;p_{ij};\dots;p_{ik};\dots;p_{m1};\dots;p_{mj};\dots;p_{mk}$

Key K: $[k_{s1};\dots;k_{sj};..;k_{sn}]$ $[k_{s1};\dots;k_{sj};\dots;k_{sn}]$ $[k_{s1};\dots;k_{sj};\dots;k_{sn}]$

CipherC: $c_{11};\dots;c_{1j};\dots;c_{1k};\dots;c_{i1};\dots;c_{ij};\dots;c_{ik};\dots;c_{m1};\dots;c_{mj};\dots;c_{mk}$

- The data stream of P is grouped into blocks having the length "*k*"
- The subgroups of *k* bits, or blocks are encrypted together:

$$\{C_{i1};\dots;C_{ij};\dots;C_{ik}\} = E(\{P_{i1};\dots;P_{ij};\dots;P_{ik}\}, Ks)$$

NORTHERN ARIZONA UNIVERSITY®

QUESTIONS ?

Dr. Bertrand Cambou
Professor of Practice NAU, Cybersecurity
School of Informatics, Computing, and Cyber-Systems
Bertrand.cambou@nau.edu