

**ALGORITHM, PROCEDURE AND DEVICE
FOR THE PROTECTION OF THE
FINANCIAL TRANSACTIONS USING
TIME STAMPING AND DATA
DELIVERED BY GALILEO**

PRESENTATION CONTENTS

- CRYPTO BASICS & PRESENT STATE
- TIME STAMPING
- GALILEO SERVICES
- GALILEO PRIVATE DATA
- ADVANTAGES OF THE PROPOSED PROCEDURE

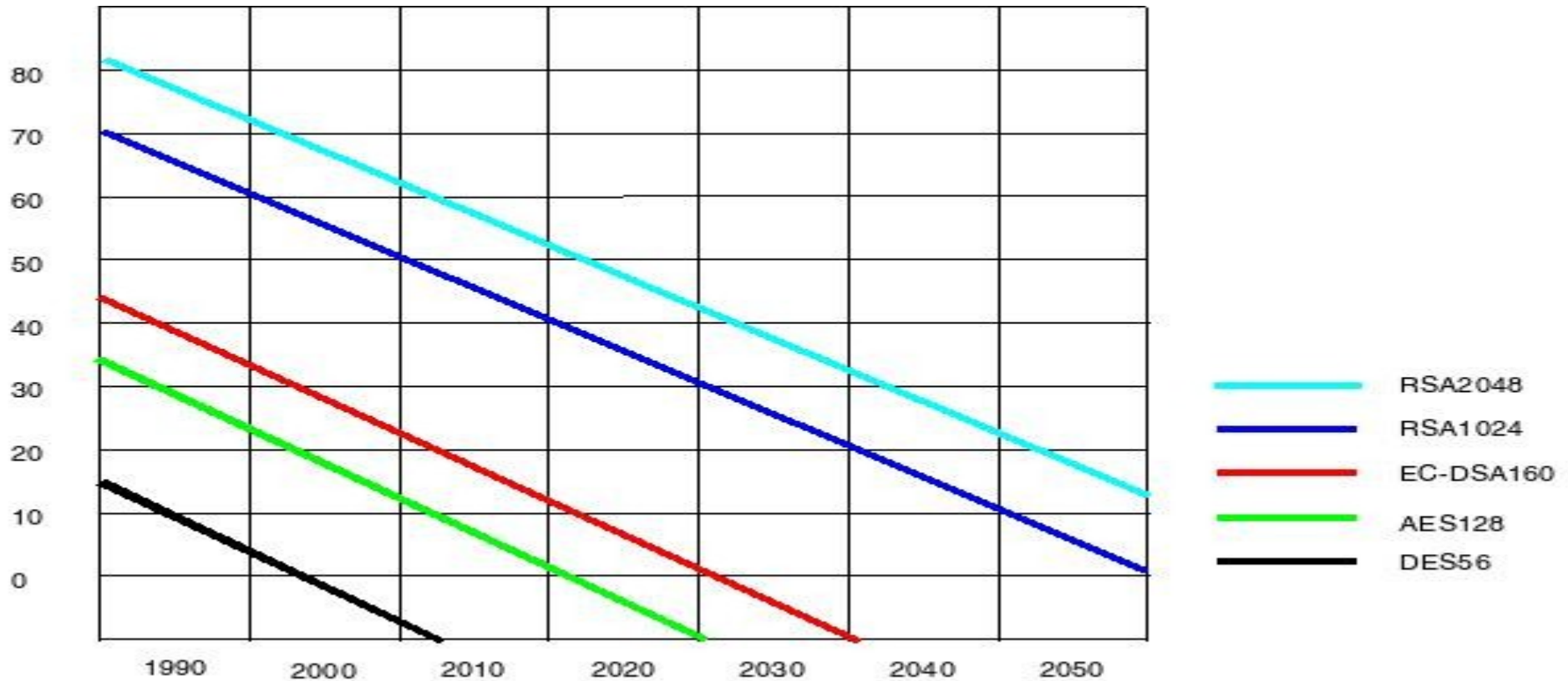
PRESENT STATE -1

- Financial transactions are performed using encryption techniques
- Several encryption algorithms are used, the most used and most known is RSA
- Moore law : Chip complexity doubles every 18 months
- Internet computing power doubles each 12 months
- For problems requiring computing power it is possible to share it
- The computer number overpassed 10k
- The power of attacks doubles each 10-12 months
- In any case, the security degree is decreasing from year to year
- The question becomes not if an algorithm will survive, but how many times

PRESENT STATE - 2

- For example, RSA key length started at 128 bits
- It was used first in 1978, in 1996 it was «broken»
- Now it is recommended to use 2048 bits or more for financial transactions
- The RSA keys need more 50 bits/year to keep constant security level
- This is true for algorithms but for «accessories» also
- Hash functions are a kind of «resumed message»
- Hash functions «lose» 2 bits de security/year

PRESENT STATE - 3



PRESENT STATE -4

- LET TAKE THE EXAMPLE OF AN CRYPTOGRAPHIC ALGORITHM
- 2500 YEARS ARE NEEDED TO «BROKE» IT ON A SINGLE COMPUTER
- THE SUPPOSED METHOD IS BASED ON THE "BRUTE FORCE"
- 2500 YEARS = 912.000 DAYS
- IF SHARED BETWEEN 1 MILION COMPUTERS
- THE COMPUTING TIME WILL BE INFERIOR OF 1 DAY
- THIS WILL BE POSSIBLE PROBABLY IN THE NEXT 3 YEARS

PRESENT SOLUTIONS

- TO USE MORE AND MORE LONGER ENCRYPTION KEYS
 - MORE TRANSMISSION TIME / HIGHER TRANSMISSION SPEEDS
 - MORE POWERFULL EQUIPEMENTS
 - MORE MEMORY NEEDS
- TO DEVELOP NEW ASYMETRICAL ENCRYPTION ALGORITHMS
- THE ELIPTYC CURVE ALGORITHM IS A GOOD EXAMPLE
- EVEN THIS ALGORITHM «LOSE» 2 BIT OF SECURITY / YEAR

TIME STAMPING

- TIME STAMPS ARE SMALL DATA BLOCKS

- A TIME INFORMATION IS CONTAINED
- IS APPENDED TO FILES OR TRANSACTIONS
- IS DELIVERED BY A TIME STAMPING AUTHORITY
- PRINCIPALLY THEY MAY NOT BE MODIFIED WITHOUT EVIDENCE
- THERE EXIST SIMPLE, LINKING AND DISTRIBUTED PROCEDURES
- SIMPLE PROCEDURES REQUIRE UNLIMITED TRUST OF TSA
- LINKING PROCEDURES LIMIT THE NEED FOR UNLIMITED TRUST
- A TIME STAMP TENTATIVE MODIFICATION REQUIRES LINKS MODIFICATION
- THE MECHANISM IS DESCRIBED BY ISO/IEC18014-3/2004 and X9.95-2005

GALILEO SERVICES

- AT THE PRESENT TIME GALILEO IS PRESUMED TO OFFER 5 SERVICES:
 - OPEN SERVICE (OS)
 - COMERCIAL SERVICE (CS)
 - SAFETY OF LIVE SERVICE (SoL)
 - PUBLIC REGULATED SERVICES (PRS)
 - SEARCH AND RESCUE (SAR) CONTRIBUTION
- NOT ALL SERVICES ARE BROADCAST BY SATELLITES
- EXAMPLE: PRECISE TIME SIGNALS
- TIME STAMPING WILL BE INCLUDED IN CS

PROPOSED SOLUTION - 1

- TO USE IN THE ENCRYPTION PROCESS TIME STAMPED ELEMENTS
- THIS IMPLIES THAT THE TRANSACTIONS VALIDITY ARE STRONGLY TIME-DEPENDENT (TIME-LIMITED)
- THE TIME STAMPED ELEMENS CONTAIN A TIME INFORMATION AND ALSO LINKS TO SOME DATA DELIVERED BY GALILEO
- THESE DATA ARE GALILEO PROPERTY, SO NOT OF PUBLIC AVAILABILITY

ADVANTAGES - 1

- ✓ THE PROPOSED PROCEDURE IS NOT ENTIRELY BASED ON MATHEMATICAL ALGORITHMS BUT PARTIALLY ON PRIVATE DATA DELIVERED BY A PHYSICAL SYSTEM (GALILEO)
- ✓ BECAUSE THE PROPOSED PROCEDURE IS ONLY PARTIALLY BASED ON MATHEMATICAL ALGORITHMS, THE PROBABILITY OF SUCCESFULL ATTACKS AGAINST IT IS LOWER
- ✓ EVEN IF THE CRYPTOGRAPHIC ALGORITHM IS « BROKEN » THE DATA WILL BE NOT DIRECTLY READABLES

ADVANTAGES - 2

- ✓ IN ORDER TO HOPE TO PERFORM A SUCCESFULL ATTACK ON THE PROPOSED ALGORITHM, IT IS NOT ENOUGH TO HAVE POWERFULL COMPUTERS AND GOOD PROGRAMMING TEAMS
- ✓ WHAT IS NEEDED IS TO ACCESS TO THE PRIVATE DATA
- ✓ THIS IS EQUIVALENT WITH THE REQUIREMENT TO MEASURE THE SAME DATA AS GALILEO, IN OTHER WORDS TO DEVELOP A NAVIGATION SYSTEM EQUIVALENT WITH GALILEO
- ✓ THE ACCES TO THIS IS STRONGLY TECHNOLOGICALLY LIMITED