

R-E-System

CRYPTOGRAPHIC SYSTEMS - CONTENTS INVENTION

In this short paper, exhibited two cryptographic non-conventional and innovative: a public key and private key to a designated either by their acronyms R-F-C A System and S.

The system was developed considering three main features:

1. Truly remarkable ensure security in communications secret of great importance;
2. ease of implementation in the short term (immediately operational);
3. low cost of implementation for deployment in various devices.

R-F-C A System – CRYPTOGRAPHY SYSTEM (PUBLIC KEY)

PROLOGUE:

The current systems such as public key: RSA, DH, Etc. elliptic curves. Based on the method of factoring large numbers on calculation or the discrete logarithm systems are theoretically and practically stick, especially for their mathematical formulation.

Require large computational resources to ensure real security, especially with age technology (progressive and growing power of processors)

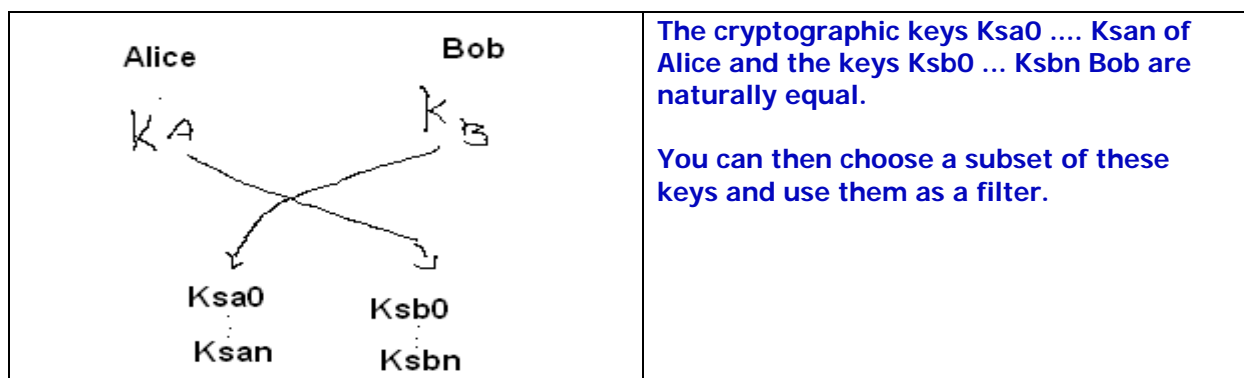
R-F-C A System, by its nature mathematics (*It does not use prime numbers as the basis for calculation*), does not grant any room for any kind of study theoretical and practical and requires low power calculation, regardless of the size of the key.

R-F-C A System was designed with the same philosophy of quantum cryptography but on a purely mathematical system that uses current technology of data, however, offering exceptional security features at low cost.

KEY FEATURES

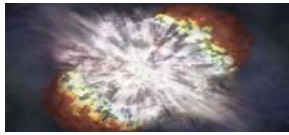
Creation of cryptographic keys:

The **R-F-C-A System** system is able to provide through *a specific mathematical function* a number of cryptographic keys theoretically infinite per user (consider each key as a single photon in a state x) as follows classic **DH**:



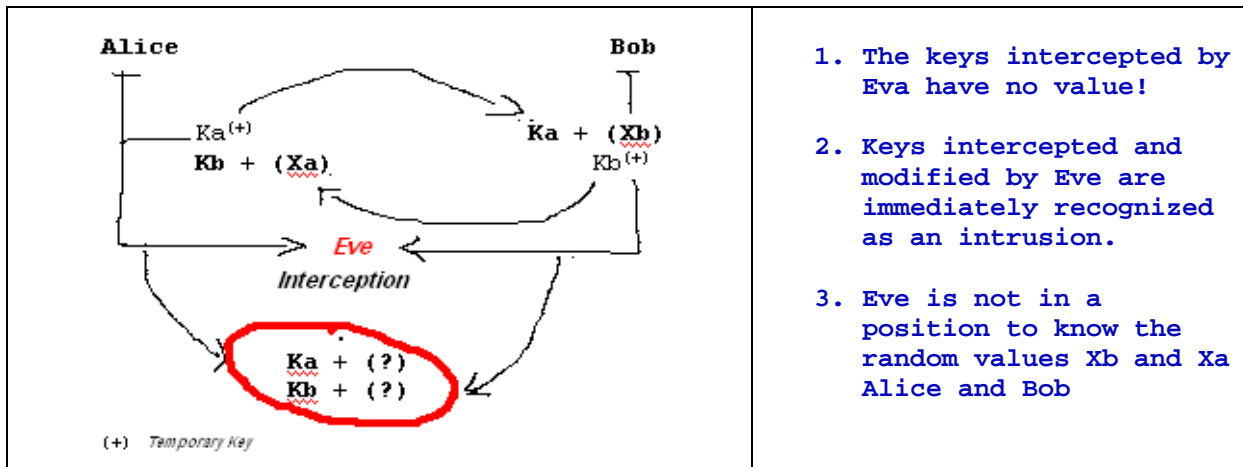
Key management:

The keys exchanged for the next phase of the cryptographic keys are storms, this means that any keys intercepted during the exchange are the keys that have no real value and thus any consideration of the same is null and void.



R-E-System

The **real keys** are composed by exploiting the legitimate communicating key time as follows:

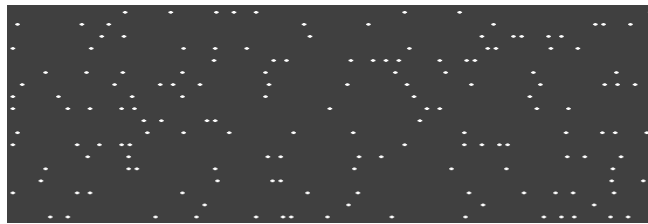


Representation of key:

the key is represented in "**Size Space Defined by Random Points**" that it is difficult to trace the real key and the information contained therein.

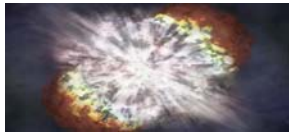
The figure represented the format is key obtained.

Example of key points defined by Random:



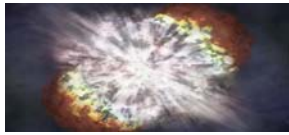
This series of random points, which are scattered in space and that have no reasonable logic, is a **key time** generated by a specific mathematical process. They contain information that only the legitimate owners and creators of the key are able to composing the real cryptographic key

FEATURES OF R-F-C-A System	
Features	Description
Length Key Private / Public	theoretically infinite
Speed	faster than at least an order of magnitude compared to the same RSA deployment HW / SW and key length
Cost deployment HW / SW time	very low compared with existing systems
Implementations	any device can support encryption (high or low power) Pc, smart card, wireless systems, telecommunications systems, special devices and satellite radio, cryptographic processors, etc ...
Type of attack	none. Only brute-force (ineffective!)
Security	high, even with the 'use of small keys (512-1024 bit)
Identification	certain and immediate according to a mechanism of mutual certification.
System symmetric key encryption combined	Whatever (Twofish, AES, R-F-C-S, etc. ...)



R-E-System

COMPARATIVE TABLE OF SYSTEMS PUBLIC KEY CRYPTOGRAPHY WITH R-F-C A System					
+/-	QKD	+/-	Public Key – RSA/DH/Elliptic Curves	+/-	Public Key R-F-C-A System
-	Requires hardware and dedicated communication lines	+	It can be implemented in Software/Hardware and portable applications	+	It can be implemented in Software/Hardware and portable devices
+	Absolutely safe because based on fundamental laws of quantum physics	-	Integrity not decided, based on mathematical known problems for which there is not a publicly known simple solution (which may, of course, exist)	+	Mathematically based on a particular function nonlinear problem for which there is no algorithm capable of obtaining the reverse.
+	QKD is secure even in the presence of quantum computers	-	Quantum computers will be able to find the keys and then break the system (see Quantum Computers for decrypting codes)	+	Very complex even for a quantum computer to break this system.
-	Brand new system and great development for the future.	+	Widespread implementation and experience with the solution.	-	Little experience thus far, but by its mathematical nature, can be seen as a guarantee an exceptional security
-	To date only works over limited distances (max 200 to 900Km) and requires direct connections with fibre optical cabling	+	It works at any distance and with any type of network	+	It works at any distance and with any type of network
-	The speed of creating key is still low (but it is growing very fast)	-	Substantial computational resources needed to ensure adequate security and is therefore liable to simple attack (very dangerous)	+	Requires low computational resources to ensure high security standards and is not subject to any known type of attack.
+	Can be easily used with a OTP (One Time Pad) algorithm that guarantees excellent security.	-	Cannot be easily used with OTP algorithms.	+	Can be easily used with OTP (One Time Pad) algorithms (indeed, specifically optimised for use with this algorithm) the only one that can guarantee today an excellent security.



R-E-System

R-F-C S CRYPTOGRAPHY SYSTEM (PRIVATE KEY)

The same considerations made for R-F-C-A System with the necessary functional differences, as in this case a private key.

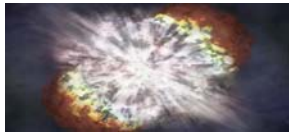
In summary:

R-F-C S is a symmetric cipher of a type that allows *FLOW* encrypt and decrypt a message in a very safe and fast.

R-F-C S basically relies on using a particular function that can create maximum entropy in bits of the message (for a process of considerable confusion) and simultaneously, through a **process of overlapping effects**, will lead to 100% the process of diffusion and confusion of bits in the message.

The choice of using one system rather than flow blocs is that the first does not have mathematical properties of large and then by its very nature is much more complex to analyze and thus to violate.

FEATURES OF R-F-C S	
Features	Description
Key Length	Up to 16,384 bits
Speed	About as fast AES
Implementation cost HW / SW time	very low compared with existing systems
Implementations	any device can support encryption (high or low power) Pc, smart card, wireless systems, telecommunications systems, special devices and satellite radio, cryptographic processors, etc ...
Type of attack	none. Only brute-force
Sub-Stream Processing (encryption / decryption)	From 64 to 2048 bits
Security	Very high, even with the 'use of small keys (128 bit)



R-E-System

NOTES:

Different organizations (no profit, from 2005) have tested this system (also, probably, NIST and NSA) Many encrypted e-mail and public key have been launched on the network to be intercepted and analyzed by several hackers.

So far I have not had any negative feedback. I personally have done tests with specific cryptanalysis software first to put other organizations.

Attack type tests: (*)

Ciphertext-only attack
Known-plaintext attack
Chosen-plaintext attack
Adaptive chosen-plaintext attack
Chosen-Ciphertext attack
Adaptive chosen-Ciphertext attack
Correlation attack
2-adic span attack
ASCII code attack
Brute force attack
Boomerang attack
Related-key attack
Slide attack
XSL attack

Cryptanalysis: (*)

Frequency analysis
Index of coincidence
Kasiski examination
Differential cryptanalysis
Impossible differential cryptanalysis
Integral cryptanalysis
Linear cryptanalysis
Mod-n cryptanalysis

(*) Attack type tests and cryptanalysis are referred only R-F-C-S, for R-F-C-A there are no actually methods of attack!

If R-F-C-S uses the special transformation technique of processing characters in points (only for very short messages, max 2-3Kb) there is no actually method of attack.

The special transformation technique of processing characters in points is very recent and is not available in current software.

The Author