

Subscribe to DeepL Pro to edit this document.  
Visit [www.DeepL.com/pro](https://www.deepl.com/pro?cta=edit-document)for more information.

Transcrypt transcendental key encryption



1. Brief history of cryptology

The need of men to communicate is at the origin of writing but the necessity appears to them almost immediately to preserve the secrecy of this writing either by hiding their messages (shorthand), or by making them incomprehensible to the uninitiated (cryptology). The two basic procedures of cryptology are transposition and substitution. Even if the "Square" of Polybre is described for the first time in -150 B.C. by the eponymous Greek historian, the foundations of the modern cipher are already laid in the 5th century B.C.

Encryption became accessible to the general public with the appearance of the first consumer computers and the crypt software (DES algorithm) of the BSD Unix operating system of the University of California at Berkeley in 1979. The first asymmetric cryptography protocols are found successively by Roger Needham-Michael Schroeder (1978) and Taher Elgamal (1984). These latter algorithms are based on highly asymmetric time (non-polynomial time or NP) to perform an inverse mathematical operation, for example decomposing a very large integer into two prime factors.

2. Problems with current encryption solutions

The difference between public-key (or asymmetric) and private-key (or symmetric) algorithms has more to do with the logistics of their implementation than with their nature. If the main measure for categorizing an encryption algorithm is its strength against cryptanalysis, it is objectively more judicious to oppose linear and non-linear algorithms.

The non-linearity and therefore the absolute inviolability of the confidentiality of an exchange are in reality non-existent without the intervention of a true stochastic process (pure chance).

One of the first weaknesses of the current public cryptology systems is that none of the proposed solutions can claim to be anything other than pseudo-random, and thus to be empirically linear, and thus to be predictable, and thus to be attackable, and thus not to ensure the confidentiality of exchanges.

Another weakness of current algorithms is that they are empirical (key sizes in number of bits increase regularly) and depend on current technologies and therefore on the evolving context of Moore's law of microprocessor speed: what is confidential one day is no longer so afterwards. Above all, these large keys are only used for practical reasons during the initial exchange of smaller keys and only hide the fragility of their respective algorithms.

A final weakness is that the vast majority of these algorithms in use are of foreign manufacture (notably the security of the Internet is based on the exclusive use of the SSL/TLS solution of the American company PKI Partners, founded by Rivest, Shamir, and Adleman), thus undermining national sovereignty.

3. Why an *n-th* encryption algorithm?

The absolute encryption algorithm consists in communicating a truly random physical band of randomness to its correspondent beforehand and encrypting the original message with this stochastic pattern by adding or superimposing it on the message, in the possession of both parties. These solutions exist but remain out of reach of the general public because they are expensive and require rigorous and heavy logistics of physical transport at the same time as a physical device of generation of randomness.

This algorithm is optimal because the algorithm is chance. It cannot be recreated by definition.

The second best solution consists in generating this true randomness (or *True number generator* TRNG in opposition to the pseudo-randomness) remotely on a computer, a means allowing a priori only the pseudo-random. Indeed, the number Pi, because of its transcendental property, allows to generate, without any additional cost linked to the physical transport or to the physical generation, a sequence of numbers without any repetition (thus with exactly the same level of entropy as the TRNG) and to infinity.

Above all, this algorithm is synonymous with a consumer solution.

Until September 19, 1995, it was impossible to implement this algorithm because to calculate the *n-th* digit after the decimal point of the number Pi, it was necessary to have previously calculated the n-1 digit. Only supercomputers could do it and the computation times were unusable.

But this has become possible since the BBP formula (or Bailey-Borwein-Plouffe formula) which allows to calculate the *n-th* digit after the decimal point of the number Pi without having to calculate the previous ones, and using very little memory and time.

4. What is **Transcrypt**?

**Transcrypt** (contraction of *Transcendental Crypting*) is a new and innovative point-to-point encryption algorithm, based on a discovery about a property of the transcendental number Pi, in 1995, by the French-Canadian mathematician Simon Plouffe.

Among the five criteria (confidentiality, integrity, availability, non-repudiation and authentication) of the security of an information system, **Transcrypt** only addresses confidentiality.

The **Transcrypt** transcendental encryption principle is the subject of a Soleau envelope deposit by Miss Alex-Pauline Poudade (national deposit number: DSO2017001085 and deposit reference 260819711812005332017) at the National Institute of Industrial Property (INPI) since February 2, 2017. Its explicit and written authorization is required for any use for profit.

**Transcrypt** is openly licensed under the Creative Commons CC-BY-NC-SA free distribution license

5. How does **Transcrypt** work?

The operation of Transcrypt is simple.

Scenario/protocol: Person A wishes to send a clear message in encrypted form to person B who replies.

1. A gets the delta of the displacement corresponding to the position of the beginning of the strip in the decimals of Pi, saved.
2. A new delta calculation for of B and applies one or exclusive XOR of the first bytes of and saves it
3. A transforms the message from binary to hexadecimal
4. A gets the length in bytes of the message
5. A obtains by BBP a strip of of length starting position
6. A applies one or exclusive XOR
7. A communicates to B
8. B gets the delta of the displacement corresponding to the position of the beginning of the strip in the decimals of Pi, saved.
9. B gets the length in bytes of the message
10. B obtains by BBP a strip of of length starting position
11. B applies one or exclusive XOR
12. B transforms the message from hexadecimal base to binary base
13. B calculates a new delta and applies one or exclusive XOR of the first bytes of and saves it
14. B gets the delta of the displacement corresponding to the position of the beginning of the strip in the decimals of Pi, saved.
15. B calculates a new delta for of A and applies one or exclusive XOR of the first bytes of and saves it
16. B transforms the message from binary to hexadecimal
17. B gets the length in bytes of the message
18. B obtains by BBP a strip of of length starting position
19. B applies one or exclusive XOR
20. B communicates to A
21. A gets the delta of the displacement corresponding to the position of the beginning of the strip in the decimals of Pi, saved.
22. A gets the length in bytes of the message
23. A obtains by BBP a strip of of length starting position
24. A applies one or exclusive XOR
25. A transforms the message from hexadecimal to binary
26. A calculates a new delta and applies one or exclusive XOR to the first bytes of and saves it

NOTE: a Proof of Concept (*POC)* in Python version 3 is provided.

6. Future and improvements of **Transcrypt** ?

Benefits:

* new and innovative system
* open source
* force does not depend on the evolution of computing power
* closest to true stochastic on automated machine
* infinite entropy (no repetition)
* the size of the keys is infinite (message size)
* one message = 1 disposable key (each key depends on the previous one)
* point-to-point (impervious to man-in-the-middle (MITM) attacks)
* does not require hashing - intrinsic integrity
* known and programmatically verifiable mathematical foundations
* national sovereignty

Current limitations:

* increase in displacement delta from 65535 to -1 (slow)
* implementation of non-cumulative travel deltas : for POC
* POC implementation in Python language to promote pedagogy
* not well suited to parallel multi-channeling (requires implementation of multi-identity management - storage of multi moves type X509/ldap)

Future improvements will concern several fields:

* filing an RFC (Request for comments) describing the operation of

Transcrypt

This will allow to useertranscrypt for public key protocols (PKI) or on IRC chat networks

* submission of an appropriate pre-publication on the ViXra website
* optimization in ANSI C language and x64 assembler

Creative Commons Attribution Noncommercial Share Alike 3.0 France

CREATIVE COMMONS CORPORATION IS NOT A LAW FIRM AND DOES NOT PROVIDE LEGAL ADVICE. THE DISTRIBUTION OF THIS LICENSE DOES NOT CREATE ANY LEGAL RELATIONSHIP BETWEEN THE PARTIES AND CREATIVE COMMONS. CREATIVE COMMONS PROVIDES THIS INFORMATION ON AN "AS IS" BASIS. CREATIVE COMMONS MAKES NO WARRANTIES REGARDING THE INFORMATION PROVIDED AND DISCLAIMS ANY LIABILITY FOR DAMAGES RESULTING FROM ITS USE.

*License*

THE WORK (AS DEFINED BELOW) IS MADE AVAILABLE UNDER THE TERMS OF THIS CREATIVE COMMONS PUBLIC LICENSE (HEREINAFTER REFERRED TO AS THE "CCP" OR "LICENSE"). THE WORK IS PROTECTED BY COPYRIGHT AND OTHER APPLICABLE LAWS. ANY USE OF THE WORK OTHER THAN AS PERMITTED BY THIS LICENSE IS RESERVED.

THE EXERCISE OF ANY RIGHT IN THE WORK MADE AVAILABLE SHALL CONSTITUTE ACCEPTANCE OF THE TERMS OF THE LICENSE. DUE TO THE CONTRACTUAL NATURE OF THE LICENSE, THE OFFEROR GRANTS THE ACCEPTOR THE RIGHTS CONTAINED IN THIS LICENSE IN CONSIDERATION OF HIS ACCEPTANCE.

1. Definitions

Adaptation: a work created either from the Work alone or from the Work and other pre-existing works. Adaptations include translations, adaptations, composite works, arrangements or modifications of a literary and artistic work, a phonogram, a videogram or an interpretation of a work, including film adaptations or any other form in which the Work may be recast, transformed or adapted, in particular any form derived from the original in an identifiable manner. For greater certainty, however, a Work that is a Collection will not be considered an Adaptation for purposes of this License. In the event that the Work is a musical creation, performance or phonogram, synchronization of the Work with a moving image will be considered an Adaptation for purposes of this License.

Collection: A collection of works which, by reason of the selection and arrangement of its contents, constitutes an intellectual creation in which each Work is included as a whole, in unaltered form, together with one or more other contributions, each of which constitutes independent and distinct works that are brought together to form that whole. Collections include, but are not limited to, encyclopedias, anthologies, performances, phonograms, videograms or broadcasts, or any work other than those designated in section 1(g). For purposes of this License, a creation that constitutes a Collection shall not be considered an Adaptation (as defined above).

Distribution: making available to the public the original version or copies of the Work or of an Adaptation, by sale or any other transfer of ownership or by any means of communication to the public insofar as these activities are sources of exclusive rights (rental, lending, etc.)

License Elements: the attributes of the License as chosen by the Licensor and listed in the title of this License: Attribution - Noncommercial - Share Alike.

Licensor: the person(s) or entity(ies) making the Work available to the public under the terms of this License.

Originating Right Holder : in the case of a literary or artistic work, the Author, understood as the natural or legal person(s) or entity(ies) who created the Work; and in addition, where applicable, (i) in the case of a performance, the actors, singers, musicians, dancers, or any other person who plays, sings, declaims or performs the literary, artistic or folkloric work; (ii) in the case of a phonogram or videogram, the producer, understood as the natural or legal person who first fixes the performance on a medium; (iii) in the case of a broadcast, the audiovisual communication undertaking that broadcasts the broadcast; (iv) in the case of a database, the producer.

Work: a creation protected by literary and artistic property law (copyright, neighbouring rights and *sui generis* rights of database producers) made available under the terms of the License. In particular, a Work may include any literary, scientific or artistic creation, regardless of the mode or form of expression, including in digital form, such as a book, pamphlet and other writings; a lecture, address, speech, course or sermon or other works of a similar nature; a dramatic work or musical; a choreographic work or pantomime; a musical composition with or without words; a work of art; a work of art; a work of art; a work of art; a musical composition with or without words; a cinematographic work to which works expressed by a process analogous to cinematography are assimilated; a drawing, painting, architectural creation, sculpture, engraving or lithography; a photographic creation to which works expressed by a process analogous to photography are assimilated; a work of applied art ; a graphic or typographical work; an illustration, map, plan, sketch or three-dimensional work relating to geography, topography, architecture or science; a performance or broadcast; a phonogram or videogram; an anthology or collection of various works or data or a database to the extent that it is protected by copyright or the right of producers of databases, provided that it is protected by the applicable law which does not cover only databases protected by copyright (for the avoidance of doubt, sections 3(a), 3(b) and 3(c) will not apply where only the right of producers of databases applies) a performance by a circus or variety artist; creations of the seasonal clothing and ornamental industries.

Acceptor: the person(s) or entity(ies) exercising the rights granted by this License in the Work and who has not previously violated the terms of this License or who has been expressly authorized by the Licensor to exercise the rights granted by this License despite a previous violation.

Representation: representation of the Work and communication to the public of such public representations by any means whatsoever, whatever the type of transmission, particularly digital, and including the modes of exploitation provided for by the applicable law. Communication to the public also includes making available protected Works in such a way that the public can access them from the place and at the time that it individually chooses, performances and communications to the public of performances of the Work, including public performances in digital format, as well as broadcasting or rebroadcasting of the Work by any means, in particular by signs, sounds or images.

Reproduction: any copy of the Work in any manner and in any form whatsoever, in particular digital and including the modes of exploitation provided for by the applicable law. A Reproduction also includes a sound or visual recording, a fixation or a reproduction of fixations of the Work, including the storage of a performance, a phonogram or a videogram in digital format or on any other electronic medium.

2. Exceptions and Limitations to Exclusive Rights. The exceptions and limitations to exclusive rights provided by applicable law are not affected by this License.

3. Scope of Authorization. Subject to the terms and conditions of this License, Offeror authorizes Acceptor to exercise, free of charge, on a non-exclusive basis, for the duration of the applicable rights protection and for the entire world, the rights to :

Reproduce, Distribute and Represent the Work, incorporate the Work into one or more Collections and reproduce the Work itself incorporated into such Collections;

Create, Reproduce, Distribute and Perform Adaptations, provided that such Adaptations, including any translation in any medium, are accompanied by appropriate labelling, demarcation or identification to make it clear that modifications have been made to the Work. For example, a translation could be labeled "The Original Work has been translated from French to English" or in the case of a modification "The Original Work has been modified";

When the Work is a database subject to the rights of database producers, extract and reuse substantial parts.

The aforementioned rights may be exercised on any media, process, technique and in any format, including, to the extent possible, future media and formats. The aforementioned rights include the right to make such modifications as are technically necessary for the exercise of these rights in other media, processes, techniques and formats. Any rights not expressly granted by the Licensor to the Acceptor in this License are reserved, in particular in the cases provided for in Section 4(f). In the event that the Offeror holds *sui generis* rights in databases under national law implementing the EU Database Directive, the Offeror waives such rights.

4. Restrictions. The authorization granted by Article 3 is expressly subject to and limited by the following restrictions:

The Acceptor may Distribute or Perform the Work only under the terms of this License. He must include a copy of this License, or his Uniform Resource Identifier (URI), with any copy of the Work he distributes or performs. The Acceptor may not offer or impose any terms of use on the Work that restrict the terms of this License or the ability of the subsequent recipient to exercise the rights granted by this License. The Acceptor may not sublicense the Work. The Acceptor must keep intact all disclaimers that refer to this License and the disclaimer of warranties with each copy of the Work that it distributes or represents. When distributing or representing the Work, the Acceptor must not impose any technological protection measure that would restrict the ability of the subsequent recipient to exercise the rights granted under this License. Section 4(a) applies to the Work as incorporated in a Collection, but does not require the Collection to be subject to the terms of this Licence. If the Acceptor creates a Collection, the Acceptor shall, at the request of any Offeror and to the extent practicable, remove from the Collection any reference to such Offeror, as provided in Section 4(d), in accordance with the request. If the Acceptor creates an Adaptation, the Acceptor shall, at the request of any Offeror and to the extent practicable, remove from the Adaptation any reference to such Offeror in the manner set forth in Article 4(d), as requested.

The Acceptor may distribute or perform an Adaptation only under the terms of: (i) this License; (ii) a later version of this License that includes the same License Elements; or (iii) a Creative Commons license that is unrestricted or restricted in any jurisdiction (in this or a later version of the License) to include the same License Elements (e.g., the "Attribution-NonCommercial-ShareAlike 3.0 Japan" License (the "Applicable License"). The Acceptor shall distribute the Adaptation under one of the licenses listed in (i), (ii) or (iii) (the "Applicable License") provided that it complies with the terms of the Applicable License generally and the following provisions:  
 The Acceptor must include a copy, or the URI, of the Applicable License with any copy of each Adaptation that it Reproduces, Distributes or Represents.  
 The Acceptor may not offer or impose any terms of use on the Adaptation that restrict the terms of the Applicable License, or the exercise of the rights granted to the recipient of the Adaptation under the Applicable License.  
 He must keep intact all disclaimers that refer to the Applicable License and the disclaimer of warranties with each copy of the work as included in the Adaptation that the Acceptor distributes or represents.  
 When the Acceptor distributes or performs an Adaptation, the Acceptor shall not impose any technological protection measure on the Adaptation that would restrict the ability of the subsequent recipient to exercise the rights granted by the Applicable License. This section 4(b) applies to the Adaptation as incorporated in a collection, but does not require that the collection apart from the Adaptation itself be subject to the terms of the applicable licence.

The Acceptor may not exercise any of the rights granted to it in Article 3 in such a way as to have the primary intention or purpose of obtaining a commercial advantage or private financial compensation. The exchange of the Work with other works subject to literary and artistic property rights by way of digital file sharing or otherwise shall not be considered as having the primary intention or purpose of obtaining a commercial advantage or private financial compensation, provided that there is no payment of financial compensation in connection with the exchange of works subject to literary and artistic property rights.

Unless a request is made under Article 4(a), the Acceptor shall, when distributing or performing the Work, or any Adaptation or Collection, keep intact all copyright notices regarding the Work and provide, in a manner appropriate to the medium or media used: (i) the name of the Original Rightsholder (or pseudonym, if any) if mentioned, and/or if the Original Rightsholder and/or the Offeror designates a party or parties (e.g., a funding agency, publisher, or newspaper) to be attributed ("the Parties to be Attributed") in the Offeror's copyright notice, terms of use, or other appropriate means, the name of the Party or Parties to be Attributed; (ii) the title of the Work, if mentioned; (iii) to the extent possible, the URI that the Offeror specifies as being associated with the Work, unless such URI does not refer to the rights notice or license information for the Work; and, (iv) in accordance with Article 3(b), in the case of an Adaptation, a statement identifying the use of the Work in the Adaptation (e.g., "French translation of the Work by the Original Rightsholder" or "script based on the Original Rightsholder's Work"). The credits required by this Article 4(d) may be implemented by any appropriate means, provided, however, that in the case of an Adaptation or Collection, such credits shall appear in a manner at least as prominent as the credits for other contributing authors, if any. For all intents and purposes, the Acceptor may use the credits required by this Article only for attribution purposes, in the manner set forth above, and in exercising the rights granted by the License. The Acceptor may not, implicitly or explicitly, state or imply any relationship, sponsorship or endorsement by the Originating Rights Holder, the Licensor, the Party or Parties to be Licensed, as the case may be, and the Acceptor or its use of the Work, without the separate, express, written and prior permission of the Originating Rights Holder, the Licensor and/or the Parties to be Licensed.

For the avoidance of doubt, the restrictions granted by Article 3 and Articles 4(a) and 4(b) are not applicable to that part of the work which is subject only to the rights of database producers.

For the avoidance of doubt:

Legal regime of compulsory collective management.   
 In cases where uses of the Work are subject to a legal system of compulsory collective management (which the law does not allow to be waived), the Offeror reserves the exclusive right to collect these royalties through the intermediary of the competent collecting society. This concerns in particular broadcasting and communication in a public place of phonograms published for commercial purposes, certain cases of cable and satellite retransmission, private copying of Works fixed on phonograms or videograms, reproduction by reprography, lending in libraries;

Mandatory Collective Management Scheme with Waiverability.   
 In jurisdictions where the right to collect royalties under any statutory licensing or compulsory collective management scheme may be waived, the Licensor reserves the exclusive right to collect such royalties arising from the exercise by the Acceptor of the rights granted under this License, provided that such rights are exercised by the Acceptor for a non-commercial purpose or use as permitted in Article 4(c), and otherwise waives the right to collect royalties under any compulsory statutory or collective management licence scheme;

Voluntary Collective Management Scheme.   
 The Licensor reserves the right to collect royalties (either individually or, if the Licensor is a member of a voluntary collective management organization, through that organization) arising from the exercise by the Acceptor of the rights granted by this License, provided that such rights are exercised for purposes or purposes other than non-commercial uses as defined in Section 4(c). For non-commercial uses as defined in Section 4(c), the Offeror waives this right.

Unless exclusive rights are limited by applicable law, if the Acceptor Reproduces, Distributes or Performs the Work itself, or as part of an Adaptation or Collection, the Acceptor must respect and not waive the moral rights of the Original Rights Owner to the extent that the Original Rights Owner benefits from such rights (such as authors and performers).

5. Representation, Warranties and Disclaimer

UNLESS OTHERWISE AGREED IN WRITING BY THE PARTIES AND WITHIN THE LIMITS OF APPLICABLE LAW, THE OFFEROR SHALL MAKE THE WORK AVAILABLE TO THE ACCEPTOR AS IS, WITHOUT REPRESENTATION OR WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE. WARRANTIES REGARDING MERCHANTABILITY, CONFORMITY, HIDDEN DEFECTS AND APPARENT DEFECTS ARE SPECIFICALLY EXCLUDED.

6. Limitation of Liability. With the exception of the public order guarantees imposed by applicable law, the Supplier shall in no case be held liable to the Acceptor, on the basis of any legal theory, for any direct, indirect, material or moral prejudice resulting from the performance of this Contract or the use of the Work, including in the event that the Supplier was aware of the possible existence of such prejudice.

7. Termination

Any breach by the Acceptor of the terms of this License shall result in automatic termination of this License and the rights hereunder. Licenses granted to individuals or entities that have received Adaptations or Collections from the Acceptor under this License will not be terminated, provided that such individuals or entities comply fully with their obligations. Sections 1, 2, 5, 6, 7 and 8 of this License shall survive termination of this License.

Subject to the above conditions, this License is granted for the full term of the copyright or other rights applicable to the Work. Notwithstanding the foregoing, the Licensor reserves the right at any time to exploit the Work under a different License or to cease Distribution at any time. However, such decision shall not result in the withdrawal of this License (or any other License that has been granted, or is to be granted, pursuant to this License), which shall continue in full force and effect unless terminated as described above.

8. Miscellaneous

When the Acceptor distributes or represents the Work or a Collection, the Offeror grants to the next beneficiary a license on the Work with the same terms and conditions as the one granted to the Acceptor.

Where the Acceptor distributes or represents an Adaptation, the Offeror shall grant the Recipient a licence to the Work on the same terms as those granted to the Acceptor.

If under applicable law any provision of this License is held to be void, invalid or unenforceable, it shall not invalidate or render unenforceable the remaining provisions of the License. Without further action by the parties, such provision shall be modified to the minimum extent necessary to make it valid and enforceable.

None of the terms or provisions of this License shall be deemed waived, and no breach shall be deemed accepted, without the written and signed consent of the party concerned.

This License represents the entire agreement between the parties with respect to the Work which is the subject of this License. There are no ancillary items, agreements or warrants relating to this Work that are not set forth above. The Offeror shall not be bound by any additional provisions that may appear in any communication from the Acceptor. This License may not be modified without the written consent of the Offeror and the Acceptor.