Create account Log in

Article Talk Read Edit View history Search

WIKIPEDIA
The Free Encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Languages
العربية
Azərbaycanca
Čeština
Deutsch
Español
فارسی
Français
Italiano
עברית
Lietuvių
Nederlands
日本語
Polski
Português
Русский
Suomi
Svenska
Türkçe
Українська
Edit links

ElGamal encryption

From Wikipedia, the free encyclopedia

"ElGamal" redirects here. For signature algorithm, see ElGamal signature scheme.

In cryptography, the **ElGamal encryption system** is an asymmetric key encryption algorithm for public-key cryptography which is based on the Diffie–Hellman key exchange. It was described by Taher Elgamal in 1985.[1] ElGamal encryption is used in the free GNU Privacy Guard software, recent versions of PGP, and other cryptosystems. The Digital Signature Algorithm is a variant of the ElGamal signature scheme, which should not be confused with ElGamal encryption.

ElGamal encryption can be defined over any cyclic group G. Its security depends upon the difficulty of a certain problem in G related to computing discrete logarithms (see below).

Contents [hide]

1 The algorithm
1.1 Key generation
1.2 Encryption
1.3 Decryption
1.4 Practical use
2 Security
3 Efficiency
3.1 Decryption
4 See also
5 References

The algorithm [edit]

ElGamal encryption consists of three components: the key generator, the encryption algorithm, and the decryption algorithm.

Key generation [edit]

The key generator works as follows:

- Alice generates an efficient description of a cyclic group G of order q with generator g. See below for a discussion on the required properties of this group.
- Alice chooses an x randomly from $\{1,\ldots,q-1\}$.
- Alice computes $h := g^x$.
- Alice publishes h, along with the description of G, q, g, as her **public key**. Alice retains x as her **private key**, which must be kept secret.

Encryption [edit]

The encryption algorithm works as follows: to encrypt a message m to Alice under her public key (G,q,g,h),

- Bob chooses a random y from $\{1,\ldots,q-1\}$, then calculates $c_1 := g^y$.
- Bob calculates the shared secret $s := h^y$.
- Bob maps his secret message m onto an element m' of G.
- Bob calculates $c_2 := m' \cdot s$.
- Bob sends the ciphertext $(c_1,c_2) = (g^y, m' \cdot h^y) = (g^y, m' \cdot (g^x)^y)$ to Alice.

Note that one can easily find h^y if one knows m'. Therefore, a new y is generated for every message to improve security. For this reason, y is also called an ephemeral key.

Decryption [edit]

The decryption algorithm works as follows: to decrypt a ciphertext (c_1,c_2) with her private key x,

- Alice calculates the shared secret $s := {c_1}^x$

- and then computes $m' := c_2 \cdot s^{-1}$ which she then converts back into the plaintext message m, where s^{-1} is the inverse of s in the group G. (E.g. modular multiplicative inverse if G is a subgroup of a multiplicative group of integers modulo *n*).

  The decryption algorithm produces the intended message, since

  $$c_2 \cdot s^{-1} = m' \cdot h^y \cdot (g^{xy})^{-1} = m' \cdot g^{xy} \cdot g^{-xy} = m'.$$

Practical use [edit]

The ElGamal cryptosystem is usually used in a hybrid cryptosystem. I.e., the message itself is encrypted using a symmetric cryptosystem and ElGamal is then used to encrypt the key used for the symmetric cryptosystem. This is because asymmetric cryptosystems like Elgamal are usually slower than symmetric ones for the same level of security, so it is faster to encrypt the symmetric key (which most of the time is quite small if compared to the size of the message) with Elgamal and the message (which can be arbitrarily large) with a symmetric cypher.

Security [edit]

The security of the ElGamal scheme depends on the properties of the underlying group G as well as any padding scheme used on the messages.

If the computational Diffie–Hellman assumption (CDH) holds in the underlying cyclic group G, then the encryption function is one-way.[2]

If the decisional Diffie–Hellman assumption (DDH) holds in G, then ElGamal achieves semantic security.[2] Semantic security is not implied by the computational Diffie–Hellman assumption alone.[3] See decisional Diffie–Hellman assumption for a discussion of groups where the assumption is believed to hold.

ElGamal encryption is unconditionally malleable, and therefore is not secure under chosen ciphertext attack. For example, given an encryption (c_1, c_2) of some (possibly unknown) message m, one can easily construct a valid encryption $(c_1, 2c_2)$ of the message $2m$.

To achieve chosen-ciphertext security, the scheme must be further modified, or an appropriate padding scheme must be used. Depending on the modification, the DDH assumption may or may not be necessary.

Other schemes related to ElGamal which achieve security against chosen ciphertext attacks have also been proposed. The Cramer–Shoup cryptosystem is secure under chosen ciphertext attack assuming DDH holds for G. Its proof does not use the random oracle model. Another proposed scheme is DHAES,[3] whose proof requires an assumption that is weaker than the DDH assumption.

Efficiency [edit]

ElGamal encryption is probabilistic, meaning that a single plaintext can be encrypted to many possible ciphertexts, with the consequence that a general ElGamal encryption produces a 2:1 expansion in size from plaintext to ciphertext.

Encryption under ElGamal requires two exponentiations; however, these exponentiations are independent of the message and can be computed ahead of time if need be. Decryption only requires one exponentiation:

Decryption [edit]

The division by s can be avoided by using an alternative method for decryption. To decrypt a ciphertext (c_1, c_2) with Alice's private key x,

- Alice calculates $s' = c_1^{q-x} = g^{(q-x)y}$.

s' is the inverse of s. This is a consequence of Lagrange's theorem, because

$$s \cdot s' = g^{xy} \cdot g^{(q-x)y} = (g^q)^y = e^y = e,$$

where e is the identity element of G.

- Alice then computes $m' = c_2 \cdot s'$, which she then converts back into the plaintext message m.

  The decryption algorithm produces the intended message, since

  $$c_2 \cdot s' = m' \cdot s \cdot s' = m' \cdot e = m'.$$

See also [edit]

- ElGamal signature scheme
- Homomorphic encryption

References [edit]

1. ^ Taher ElGamal (1985). "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms" (PDF). *IEEE Transactions on Information Theory* **31** (4): 469–472. doi:10.1109/TIT.1985.1057074. (conference version appeared in CRYPTO'84, pp. 10–18)
2. ^ *a b* *CRYPTUTOR*, "Elgamal encryption scheme"
3. ^ *a b* M. Abdalla, M. Bellare, P. Rogaway, "DHAES, An encryption scheme based on the Diffie–Hellman Problem" (Appendix A)

- ElGamal, Taher (1985). "A public key cryptosystem and a signature scheme based on discrete logarithms" (PDF). *Advances in cryptology: Proceedings of CRYPTO 84*. Lecture Notes in Computer Science **196**. Santa Barbara, California, United States: Springer-Verlag. pp. 10–18. doi:10.1007/3-540-39568-7_2.
- A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. "Chapter 8.4 ElGamal public-key encryption". *Handbook of Applied Cryptography* (PDF). CRC Press.
- Dan Boneh (1998). "The Decision Diffie–Hellman Problem". *Lecture Notes in Computer Science* **1423**: 48–63. doi:10.1007/BFb0054851.

v · t · e	**Public-key cryptography**
Algorithms	AEDH · Benaloh · Blum–Goldwasser · Cayley–Purser · CEILIDH · Cramer–Shoup · Damgård–Jurik · DH · DSA · EPOC · ECDH · ECDSA · EdDSA · EKE · **ElGamal** (signature scheme) · GMR · Goldwasser–Micali · HFE · IES · Lamport · McEliece · Merkle–Hellman · MQV · Naccache–Stern · Naccache–Stern knapsack cryptosystem · NTRUEncrypt · NTRUSign · Paillier · Rabin · RSA · Okamoto–Uchiyama · Schnorr · Schmidt–Samoa · SPEKE · SRP · STS · Three-pass protocol · XTR
Theory	Discrete logarithm · Elliptic curve cryptography · Non-commutative cryptography · RSA problem
Standardization	CRYPTREC · IEEE P1363 · NESSIE · NSA Suite B
Topics	Digital signature · OAEP · Fingerprint · PKI · Web of trust · Key size

v · t · e	**Cryptography**
History of cryptography · Cryptanalysis · Cryptography portal · Outline of cryptography	
Symmetric-key algorithm · Block cipher · Stream cipher · Public-key cryptography · Cryptographic hash function · Message authentication code · Random numbers · Steganography	

Categories: Public-key encryption schemes