(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
15 juin 2006 (15.06.2006)

PCT

(10) Numéro de publication internationale
WO 2006/061420 A1

(51) Classification internationale des brevets :
H04L 9/08 (2006.01) *H04L 9/30* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2005/056613

(22) Date de dépôt international :
8 décembre 2005 (08.12.2005)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
04292975.2 10 décembre 2004 (10.12.2004) EP

(71) Déposant *(pour tous les États désignés sauf US)* : **NAGRA FRANCE SARL** [FR/FR]; Rue Du Colonel Pierre Avia, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **NIMOUR, Abdelkrim** [DZ/FR]; Rue De Fontenay 31, F-92320 Chatillon (FR). **BARBIER, Eve-Marie** [FR/FR]; Bat. A, Appart.16, Av. Léonard De Vinci 51, F-92400 Courbevoie (FR). **BREDY, Nicolas** [FR/FR]; Boulevard D'alembert 8, F-78180 Montigny-le-bretonneux (FR).

(74) Mandataire : **NITHARDT, Joël**; Leman Consulting S.A., Route De Clémenty 62, CH-1260 Nyon (CH).

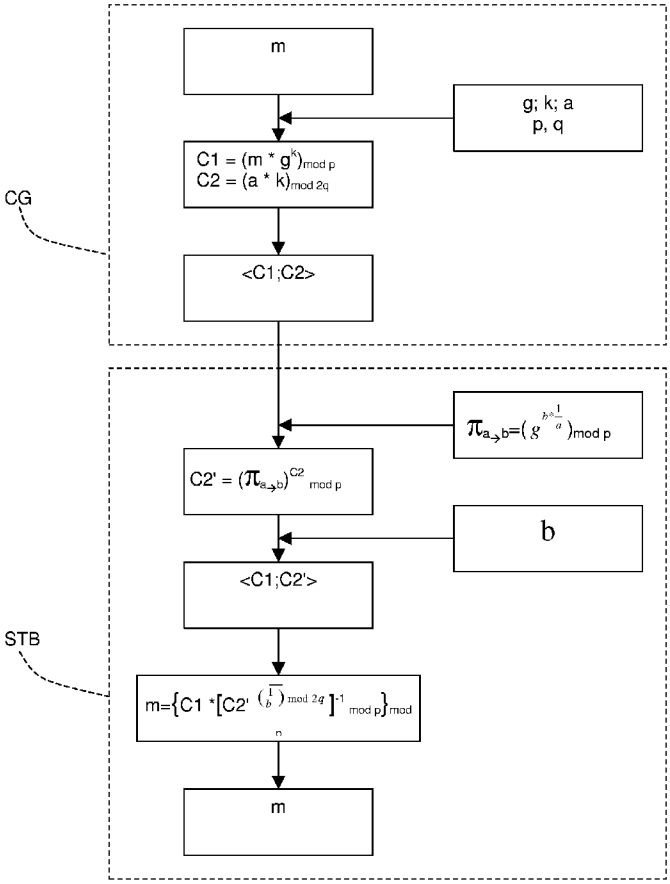
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY,

[Suite sur la page suivante]

WO 2006/061420 A1

(54) **Title:** METHOD AND SYSTEM FOR ENCRYPTION BY A PROXY

(54) **Titre :** PROCEDE ET SYSTEME D ' ENCRYPTION PAR UN PROXY



(57) Abstract: The invention concerns a method for transmitting messages between a transmitter and at least one receiver, comprising the following steps: encrypting the message (m) to be transmitted using a key (a) associated with said transmitter; sending the encrypted message in a conversion module comprising a conversion key ($\pi_{a\to b}$) and a conversion function; converting the encrypted message received in the conversion module into an encrypted message capable of being decrypted by a key (b) specific to said receiver, said conversion being carried out without the initial message appearing in plain text in the conversion module; sending the converted message to said receiver; decrypting said transformed message received by said receiver using the specific key (b). The invention is characterized in that the conversion key ($\pi_{a\to b}$) of the conversion module depends on a non-trivial value exponentiated to the value of the key (a) related to the transmitter and the key (b) related to the receiver. The invention also concerns a system for transmitting messages between a transmitter and at least one receiver, said system being configured to implement the inventive method.

(57) Abrégé : La présente invention concerne un procédé de transmission de messages entre un émetteur et au moins un récepteur, comportant les étapes suivantes : - chiffrement du message (m) à transmettre au moyen d'une clé (a) associée audit émetteur; - envoi du message chiffré dans un module de conversion comportant une clé de conversion ($\pi_{a\to b}$) et une fonction de conversion; - conversion du message chiffré reçu dans le module de conversion en un message chiffré de façon

[Suite sur la page suivante]

MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

à pouvoir être déchiffré par une clé (b) spécifique audit récepteur, cette conversion étant effectuée sans que le message initial n'apparaisse en clair dans le module de conversion; - envoi du message converti audit récepteur; - déchiffrement dudit message transformé reçu par ledit récepteur au moyen de la clé spécifique b; caractérisé en ce que la clé de conversion ($\pi_{a\to b}$) du module de conversion dépend d'une valeur non triviale élevée à une puissance de la clé (a) liée à l'émetteur et de la clé (b) liée au récepteur. Cette invention concerne également un système de transmission de messages entre un émetteur et au moins un récepteur, ce système étant agencé pour mettre en oeuvre le procédé de l'invention.