PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/32 — A1

(11) Numéro de publication internationale: WO 00/10287

(43) Date de publication internationale: 24 février 2000 (24.02.00)

(21) Numéro de la demande internationale: PCT/FR99/01995

(22) Date de dépôt international: 16 août 1999 (16.08.99)

(30) Données relatives à la priorité:
98/10591 17 août 1998 (17.08.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: GEMPLUS S.C.A. [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(72) Inventeur; et

(75) Inventeur/Déposant *(US seulement)*: ROUSSEAU, Ludovic [FR/FR]; Bâtiment A, Les Aires Saint Michel, F–13400 Aubagne (FR).

(74) Mandataire: NONNENMACHER, Bernard; Gemplus S.C.A., Avenue du Pic de Bertagne, Parc d'Activités de Gémenos, F–13881 Gémenos Cedex (FR).

(81) Etats désignés: AU, CA, CN, IN, JP, MX, SG, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD AND DEVICE FOR AUTHENTICATING WITH SYMMETRICAL ALGORITHM

(54) Titre: PROCEDE ET DISPOSITIF D'AUTHENTIFICATION A ALGORITHME SYMETRIQUE

(57) Abstract

The invention concerns a method and a system for authenticating with symmetrical algorithm essentially characterised in that, for each mutual authentication of two parties, a cryptographic computation with a variable key, referred to as K', is carried out. The main steps of said method are as follows: a) party A, possessing the secret key K, sends a random number R_1 to party B; the latter also possessing the same secret key K; b) party B selects a random number R_2 and computes the number K', which is also a secret key, from the following formula: $K' = R_2$ xor K, xor being the equivalent of the exclusive or mathematical operation; c) then, B, using a symmetrical encryption algorithm ALG, computes a result r derived from the formula: $r = ALG[K'](R_1)$; d) said party B then sends r and R_2 to said party A; e) said party A, using the same symmetrical encryption algorithm ALG, computes K' and r' from the following formulae: $K' = R_2$ xor K and $r' = ALG[K'](R_1)$; f) if r is equal to r', then said party B is authenticated by said party A.

(57) Abrégé

La présente invention concerne un procédé et un système d'authentification à algorithme symétrique présentant la caractéristique principale que, à chaque authentification de deux parties entre elles, un calcul cryptographique avec une clé variable, appelée K', est effectué. Les principales étapes du procédé de l'invention sont les suivantes: (a) la partie A, possédant la clé secrète K, envoie un aléa R_2 à la partie B, cette dernière possédant également la même clé secrète K; (b) la partie B choisit un nombre aléatoire R_2, et calcule le nombre K', qui est aussi une clé secrète, à partir de la formule suivante: $K' = R_2$ xor K, xor étant l'équivalent du "ou exclusif" mathématique; (c) ensuite, B calcule, à l'aide d'un algorithme symétrique de chiffrement ALG, un résultat r issu de la formule: $r = ALG[K'] (R_1)$; (d) ladite partie B envoie ensuite r et R_2 à ladite partie A; (e) ladite partie A calcule, à l'aide du même algorithme symétrique de chiffrement ALG, K' et r' à partir des formules suivantes: $K' = R_2$ xor K et $r' = ALG[K'] (R_1)$; (f) si r est égal à r', alors ladite partie B est authentifiée par ladite partie A.