

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2006 年 7 月 13 日 (13.07.2006)

PCT

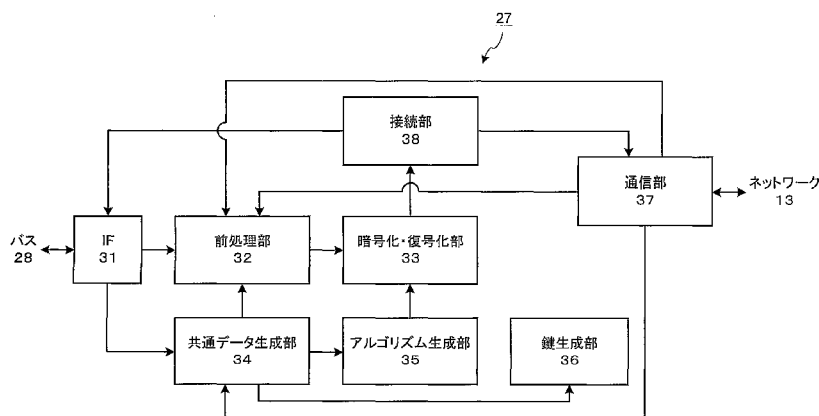
(10) 国際公開番号
WO 2006/073200 A1

- (51) 国際特許分類:
H04L 9/16 (2006.01) H04L 9/08 (2006.01)
G09C 1/04 (2006.01)
- (21) 国際出願番号: PCT/JP2006/300158
- (22) 国際出願日: 2006 年 1 月 4 日 (04.01.2006)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2005-003259 2005 年 1 月 7 日 (07.01.2005) JP
- (71) 出願人 (米国を除く全ての指定国について): 株式会社エヌクリプト (N-CRYPT, INC.) [JP/JP]; 〒5128044 三重県四日市市中村町 2 2 9 3 番地 1 Mic (JP).
- (72) 発明者; および
- (75) 発明者/出願人 (米国についてのみ): 中村 貴利 (NAKA-MURA, Takatoshi) [JP/JP]; 〒5128044 三重県四日市市中村町 2 2 9 3 番地 1 株式会社エヌクリプト内 Mic (JP).
- (74) 代理人: 鈴木 正剛, 外 (SUZUKI, Seigoh et al.); 〒1050014 東京都港区芝三丁目 2 2 番 7 号 芝 N K ビル 4 階 Tokyo (JP).
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, 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) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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),

[続葉有]

(54) Title: COMMUNICATION SYSTEM AND COMMUNICATION METHOD

(54) 発明の名称: 通信システム、通信方法



28... BUS
32... PREPROCESSING PART
34... COMMON DATA GENERATING PART
38... CONNECTING PART
33... ENCRYPTING/DECRYPTING PART
35... ALGORITHM GENERATING PART
36... KEY GENERATING PART
37... COMMUNICATING PART
13... NETWORK

(57) Abstract: A communication system including two communication apparatuses is improved such that the possibility that a third party decrypts the communication is reduced. A communication system includes first and second communication apparatuses, one of which encrypts data to be transmitted and transmits the encrypted data to the other communication apparatus, which receives and decrypts the encrypted data. Each communication apparatus generates an algorithm to be used for encryption each time it performs an encryption or decryption. In this case, each communication apparatus generates a new algorithm by assigning a past solution to a solution generation algorithm that allows the new algorithm to be generated. The past solution, when having become unused, is erased.

[続葉有]

WO 2006/073200 A1



OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML,
MR, NE, SN, TD, TG).

2文字コード及び他の略語については、定期発行される
各PCTガゼットの巻頭に掲載されている「コードと略語
のガイダンスノート」を参照。

添付公開書類:

— 国際調査報告書

(57) 要約:

2つの通信装置を含む通信システムを、第三者による通信の解読の可能性をより小さくするように改良する。

通信システムは、第1通信装置と第2通信装置を含み、一方の通信装置で送信対象データを暗号化して生成した暗号化データを他方の通信装置に送信し、その他方の通信装置で、受取った暗号化データの復号化を行う。各通信装置は、暗号化又は復号化を行うごとに暗号化に用いるアルゴリズムを生成する。この場合、各通信装置は、過去の解を代入することによって新しいアルゴリズムを生成することのできる解生成用アルゴリズムに、過去の解を代入してアルゴリズムを生成する。過去の解は使用されなくなった時点で消去される。