(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2006 年9 月14 日 (14.09.2006)

PCT

(10) 国際公開番号
WO 2006/095895 A1

(51) 国際特許分類:
H04L 9/06 (2006.01) *H04L 9/28* (2006.01)
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2006/304836

(22) 国際出願日: 2006 年3 月7 日 (07.03.2006)

(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2005-063270 2005 年3 月8 日 (08.03.2005) 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２２９３番地１ Mie (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 (NAKAMURA, Takatoshi) [JP/JP]; 〒5128044 三重県四日市市中村町２２９３番地１ 株式会社エヌクリプト内 Mie (JP).

(74) 代理人: 鈴木 正剛, 外(SUZUKI, Seigoh et al.); 〒1050014 東京都港区芝二丁目２９番１０号 パシフィックシティ芝ビル６階 Tokyo (JP).

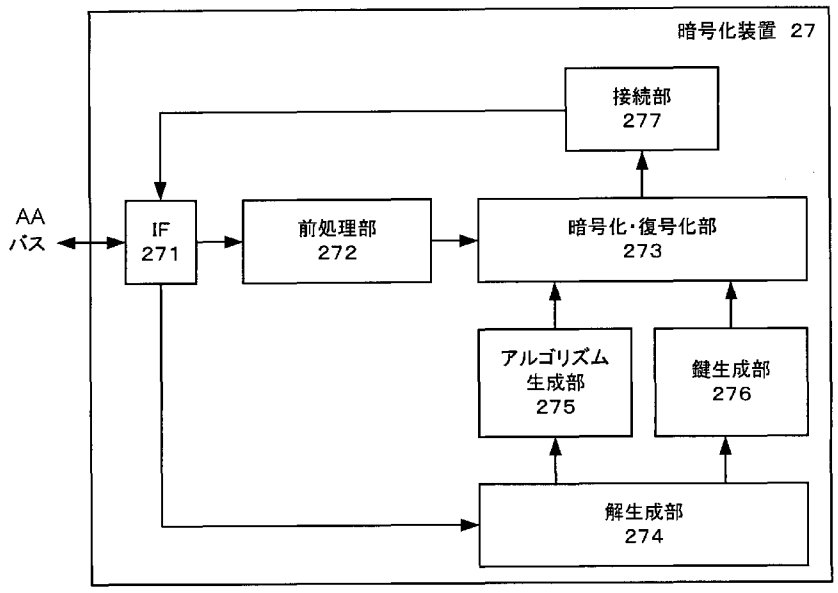
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, 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,

[続葉有]

(54) **Title:** DATA PROCESSING APPARATUS

(54) 発明の名称: データ処理装置



AA.. BUS
272. PRE-PROCESSING PART
27.. ENCRYPTING APPARATUS
277. CONNECTING PART
273. ENCRYPTING/DECODING PART
275. ALGORITHM GENERATING PART
276. KEY GENERATING PART
274. SOLUTION GENERATING PART

(57) **Abstract:** To improve the encryption technique in a data processing apparatus such that the possibility of communication decryption by a third party is reduced. A data processing apparatus wherein data, which is to be processed, is encrypted to provide encrypted data; this encrypted data is then recorded into a predetermined recording medium; and the encrypted data recorded in the recording medium is decoded to reproduce the data to be processed. During the encryption, the data to be processed is divided into predetermined bits of divisional plaintext data, and then each divisional plaintext data is encrypted. At this moment, the numbers of bits of the divisional plaintext data are varied, while dummy data is mixed into the divisional plaintext data other than the one having the largest number of bits. In this case, the dummy data has the same number of bits as the divisional plaintext data having the largest number of bits.

[続葉有]

WO 2006/095895 A1

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

添付公開書類:
— 国際調査報告書

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。

(57) 要約: データ処理装置における暗号化の技術を、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。 データ処理装置は、処理対象データを暗号化して暗号化データとし、それを所定の記録媒体に記録するようになっているとともに、記録媒体に記録したその暗号化データを復号化して処理対象データに戻すようになっている。暗号化は、処理対象データを所定のビット数毎に切断して生成した平文切断データを単位として行うが、その際に、平文切断データのビット数に変化をつけるとともに、平文切断データのうち最もビット数の大きいもの以外の平文切断データに、最もビット数の大きいものにそのビット数を合わせる大きさのダミーデータを混入する。