暗号とは

○○しないで，
□□する．

特定の計算の実行が，特定の知識が利用できる場合には効率よく行え，利用できない場合には極めて困難であるように制御する情報処理技術の総称．

特定の者だけに通信文の内容を伝える守秘機能や，通信文の作成または変更を行ったのが特定の者であるか否かを確認する認証機能などの，さまざまな情報セキュリティ機能を提供する．（電子情報通信用語辞典，コロナ社，1999）

例えば：

特定の計算の実行（暗号文を通信文に戻す変換）が，特定の知識（鍵の値）が利用できる場合には効率よく行え，利用できない場合には極めて困難であるように制御する．

経営学の観点からすると，低いコストで高度のセキュリティが実現できることが重要である。

用語

鍵	Key
通信文（平文の）	Message
↓暗号化	Encryption
暗号文	Cryptogram
↓復号	Decryption
↓解読	cryptanalysis
通信文	

暗号解読の段階（困難な順）

(1) 暗号文だけによる攻撃
(2) 既知の平文による攻撃 …… ここまでは耐えるべき
(3) 任意の平文による攻撃

本国 ＝＝ 大使館 —— 支局

右側の弱い回線が破られていると，(2) が可能になる.

暗号機が敵に入手されると，(3) が可能になる.

★ 解読に成功しても，その事実は隠そうとする.

おちゃ混ぜクイズ：

ザ・ウドンリキ

RSA 方式

公開鍵暗号を実現する方式の一つ．非常に大きな 2 素数の積 n の因数分解が極めて困難なことを利用している．1977 年に Rivest，Shamir，Adleman の 3 名が考案した．

暗号化： $C = M^e \mod n$

復号： $M = C^d \mod n$

$$C^d = (M^e)^d = M^{ed} \equiv M \pmod{n}$$