演習のTheme（各テーマ3グループまで）

1. 楕円暗号方式（ECDSA/EdDSA）ってなに？RSAとどう違う？
2. エニグマをつくる
3. GDPR（General Data Protection Regulation）って？？
4. 中国におけるネットワークセキュリティ5大脅威
5. 大根？写真？グミの指紋？生体認証とその弱点
6. CTF(Capture the flag) に挑戦してみた
7. 魔法の言葉は気難しいヒゲワシ（素因数分解）を解いてみた。（もっと大きい素因数分解にもチャレンジしてみた）
8. 乱数を作ってみた（擬似乱数とハードウェア乱数について）
9. （自由テーマ）: 自由にThemeを決めていい。でも、必ずメールで問い合わせてください

ネットワークセキュリティ：Network security

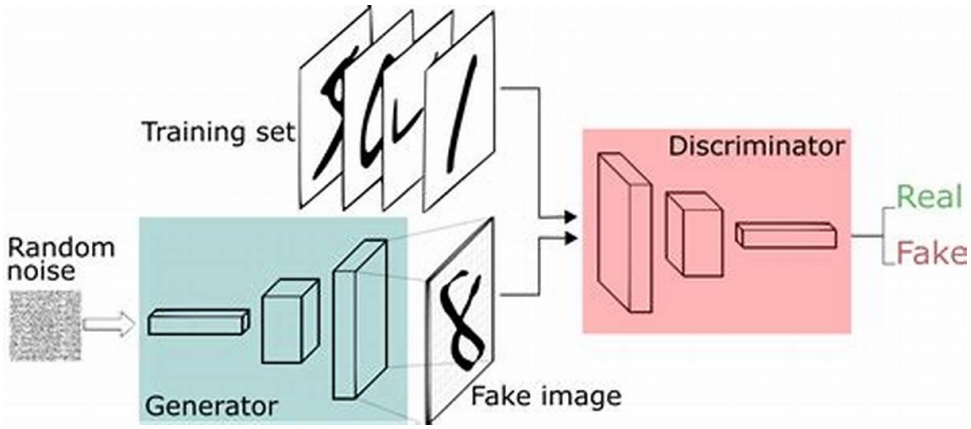
暗号（1）
—Introduction—

野口　拓
Taku NOGUCHI

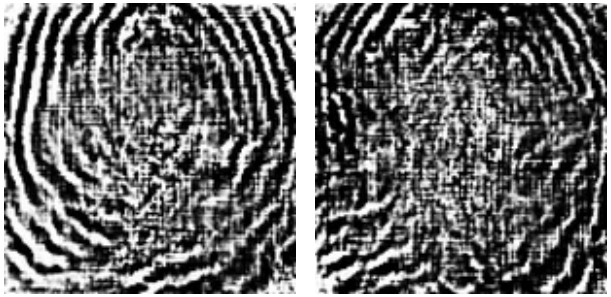
深層学習と情報セキュリティ
Deep learning and Information Security

- GAN (Generative Adversarial Network、敵対的学習)
- 騙し、騙されを繰り返すことで良いものを生成する方法

マスターキー：master key



指紋のマスターキーをつくる研究



Bontrager et al., DeepMasterPrints: Generating MasterPrints for Dictionary Attacks via Latent Variable Evolution, https://arxiv.org/abs/1705.07386

暗号と認証：情報セキュリティの基礎技術

- 主にインターネット上で行われる通信において・・・
  - 自分が誰であるか、を、伝える
  - 相手が誰であるか、を、確認する

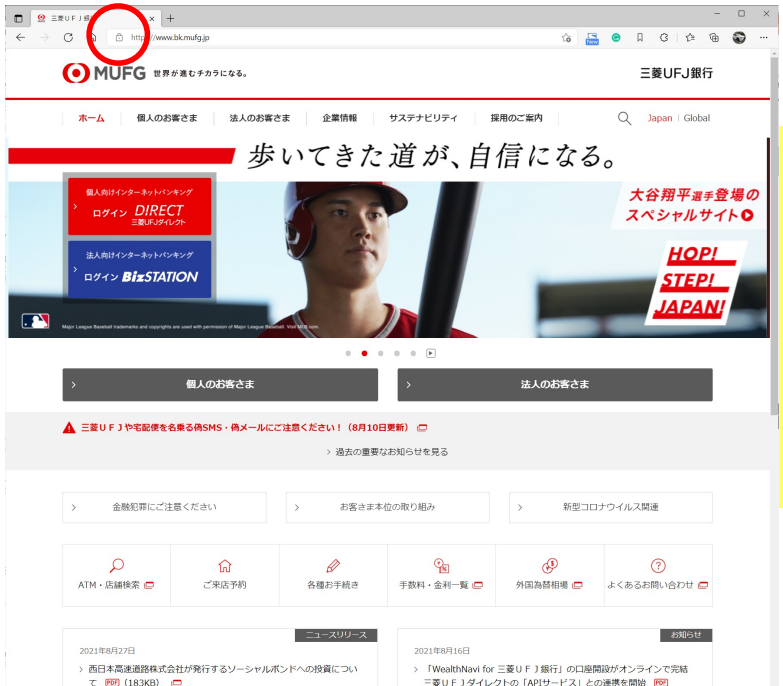
認証

- 自分と相手のやり取りを
  他の人に（不用意に）聞かれないようにする

暗号

「暗号」:騙されやすいもの

- よく見かけるメッセージ
  「お客様の個人情報は、SSLによって
  暗号化されます。ご安心下さい。」
- 実は暗号は時々破られる
  - 一瞬にして無線LANのWEPを解読する方法が登場



暗号の正しい理解は　利用のために欠かせない
「本当に安全なのか」「どうやって安全性を判断するのか」

復習をかねて：暗号とは

- 通信やデータ保存などにおいてデータが第三者に読まれない（読まれても内容がわからない）ようにする手法
- 古典暗号
  - 隠語：合言葉や置き換え語による
  - 換字式暗号：シーザー暗号など、文字を置き換える
  - 転置式暗号：文字の順番の入れ替え

シーザー：Caesar

  - 古典暗号は暗号化の方式が判明すると容易に解読される場合が多い
    →現代暗号は「暗号化方式」だけでは解読できない耐性を求められる


KEUSTUNHA

代表的古典暗号:
換字式暗号・転置式暗号

ロゼッタストーン：Rosetta Stone

アルファベット：Alphabet

ロゼッタストーンの解読

- シーザー暗号：代表的な換字式暗号
  - アルファベットで何文字かずらす
  - 例：I LOVE YOU → K NQXG AQW
  - 固定した換字表による暗号は容易に解読可能
    - “E”が多いことを利用する/1文字の単語は・・・

ら

- スキュタレー暗号(スパルタの暗号)：転置式暗号の一つ

スキュタレー：Scytale

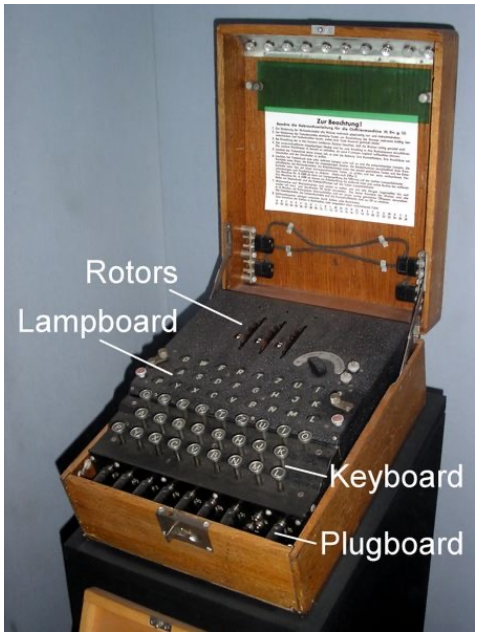
リボン：Ribbon

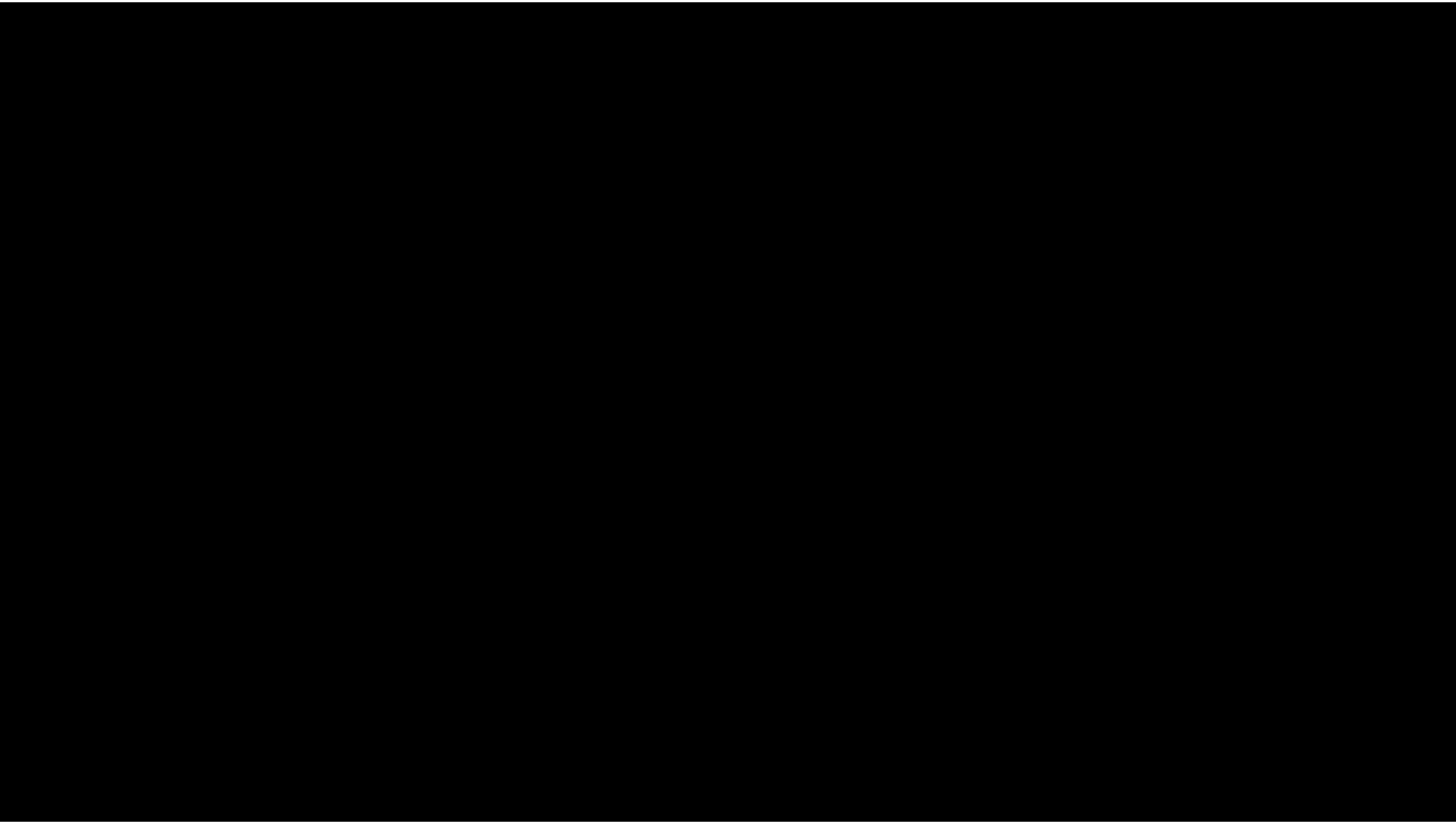
棒にリボンをまいて
そこに文字を書く
広げると文字順が
かわっている
棒の太さが「鍵」

エニグマ：Enigma

換字式暗号の化け物：エニグマ

- 第2次大戦でドイツ軍が使用したもの
  - 換字を7回繰り返す/一文字打つごとに組み合わせ変更
    - 3つの可変な換字表を正逆2回ずつと固定の換字表を利用
  - 最初の3つの換字表のパターンを決める値が鍵となっている
    （26^3通りの初期値がある）
    後に固定部分がさらに変更可能に
  - 暗号文をもう一度打ち込むと元に戻る
  - ネット上にエミュレータが沢山あります
    - http://enigmaco.de/enigma/enigma.html
  - イギリスの天才数学者チューリングにより解読される





Imitation Gameという映画がある

エニグマ：Enigma

換字式暗号を突き詰めると・・・

- バーナム暗号：「何文字ずらす」かを全ての文字について変えて送る
  - 「ずらす」割合が完全にランダムなら総当たりによってしか解読できない

平文：I LOVE YOU

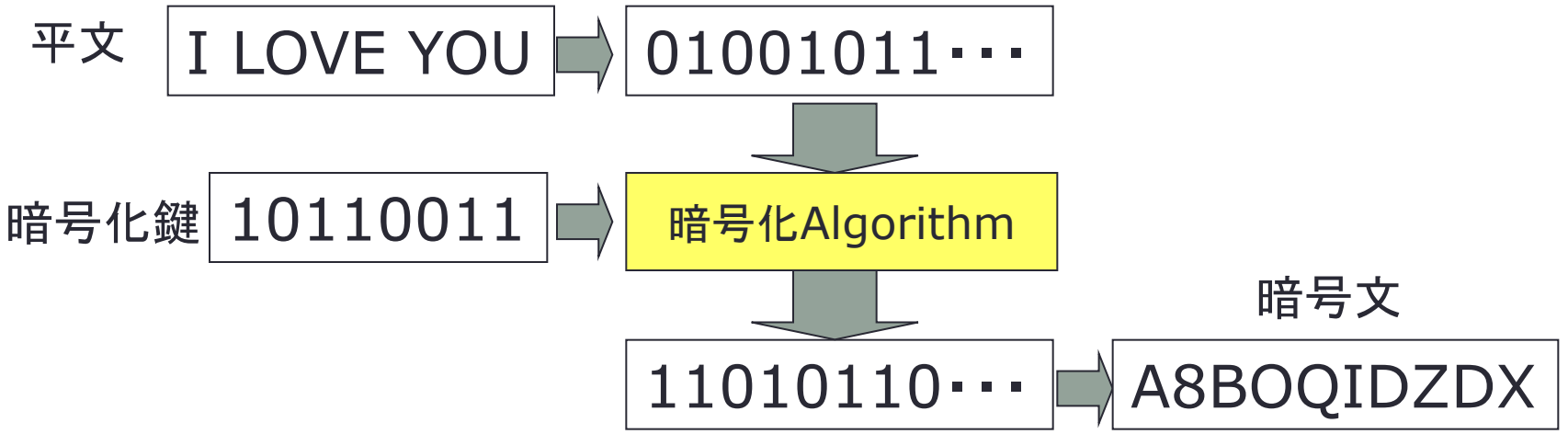
鍵：2-11-6-3-0-23-14-8　←これがRandom

暗号文：K WUYE VCC

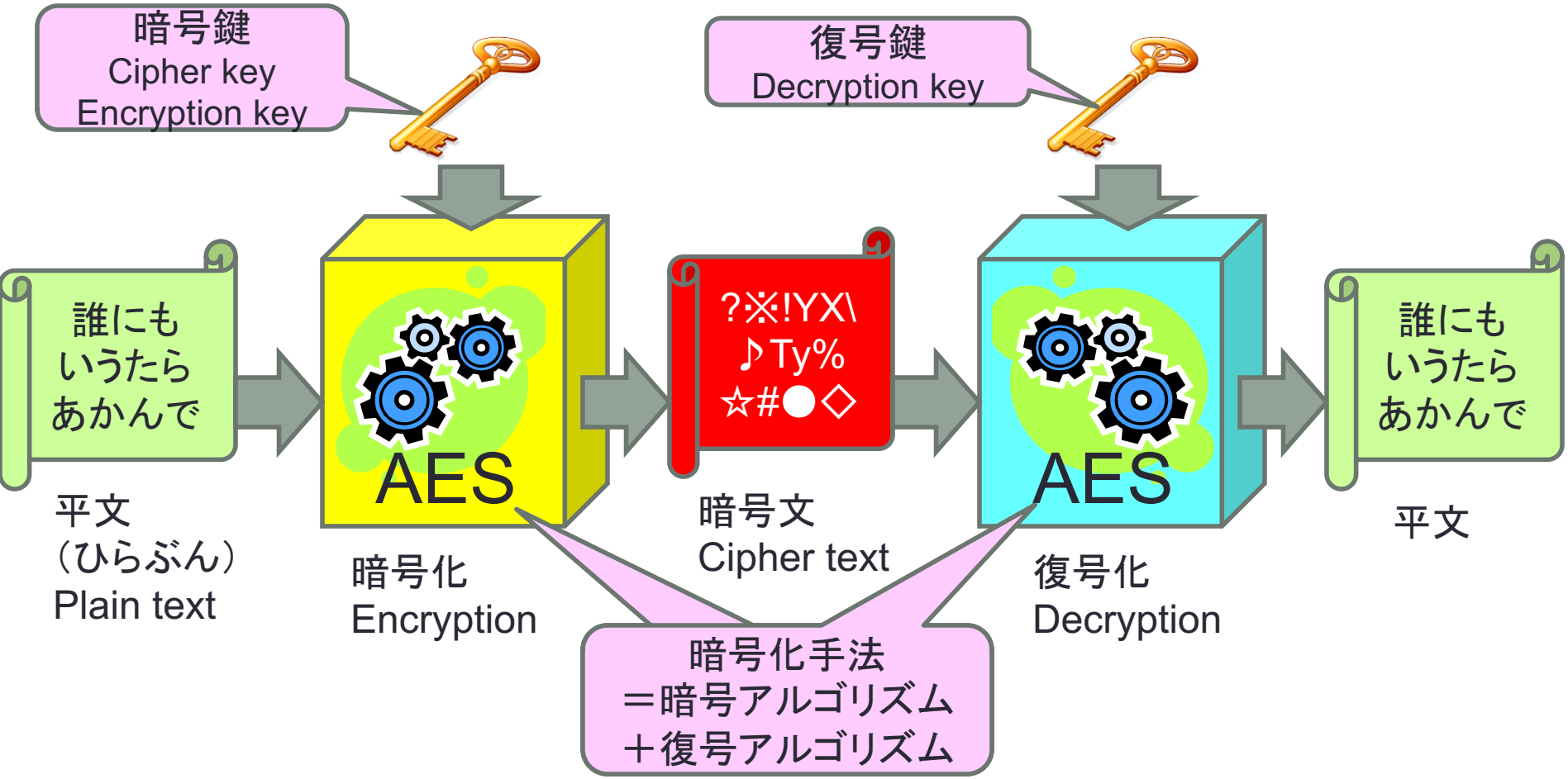
- だが鍵が平文と同じ長さになってしまうのでほとんどの場合は現実的でない

現代暗号の基礎

- computer（Computer:電脳）が前提
- computerの世界では全てのDataは（文字も含め）2進数で表現される
- 2進数列と鍵とから別の2進数列を作るのが暗号である
- この状態であらゆる攻撃に耐える必要がある

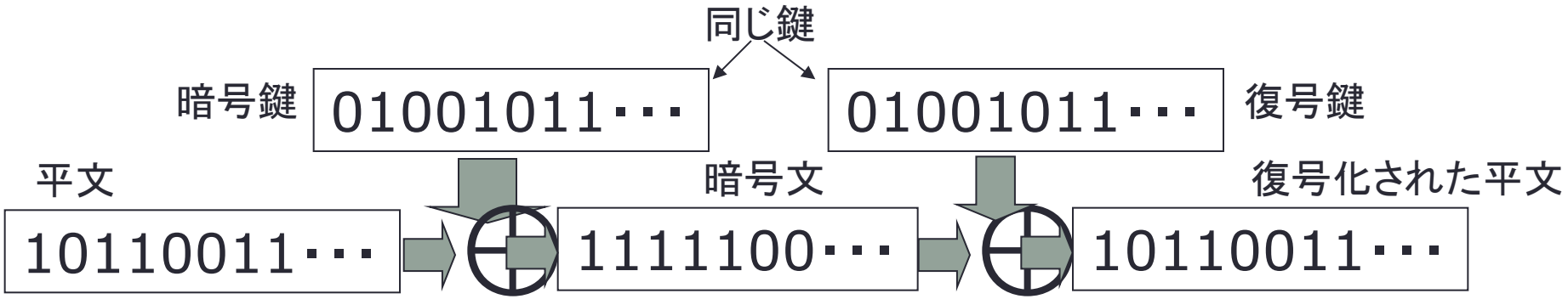


暗号(Cipher)の基本用語



Stream暗号

- Stream暗号：任意bit長の平文を暗号化
  - XOR:排他的論理和を使う
    0⊕0=0 0⊕1=1 1⊕0=1 1⊕1=0
  - 平文と同じ長さの鍵とXORする
  - 鍵が真に乱数なら情報理論的に安全
  - しかし鍵を真に乱数にすることは困難
    - 毎回平文ごとに違う乱数を作る必要がある
    - しかも平文と同じ長さの鍵を安全に送れるか・・・？
  - 普通は擬似乱数を使う：擬似乱数の「種」が鍵になる
  - 処理に遅延が小さいのが大きな特徴
    - RC4:無線LANのWEPで使われている暗号化アルゴリズム



擬似乱数列生成機

- シードseed（種）を与えると、乱数列を生成する

- 二乗中抜き法（Neumann）
- 線形合同法
- メルセンヌツイスター

  Mersenne twister

例：二乗中抜き法
ある数を二乗して、その間の数をとり乱数とする

初期値＝1234

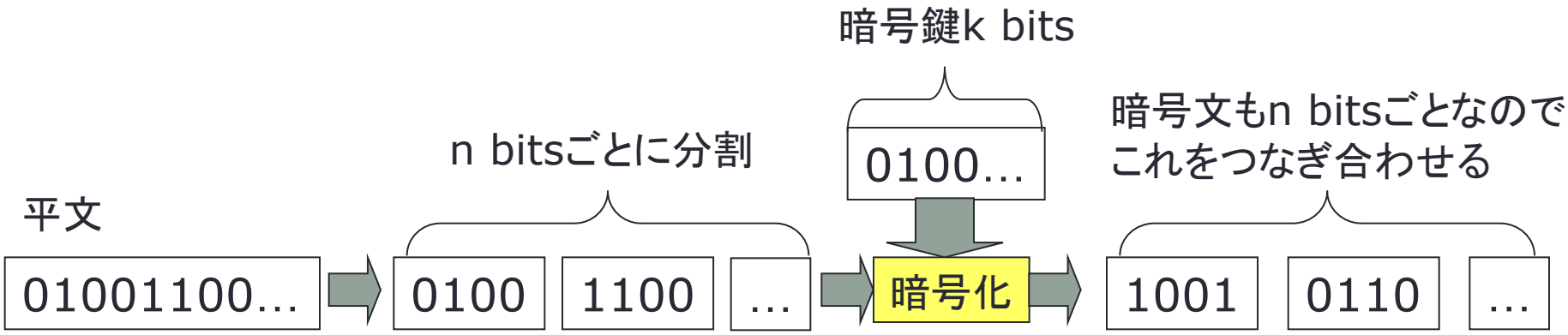
1234^2= 01522756
5227^2= 27321529
3215^2=10336225
3362^2=11303044
3030^2=09180900

5227321533623030 1809…..

初期値によって次に生成される数列が決まる

Block暗号

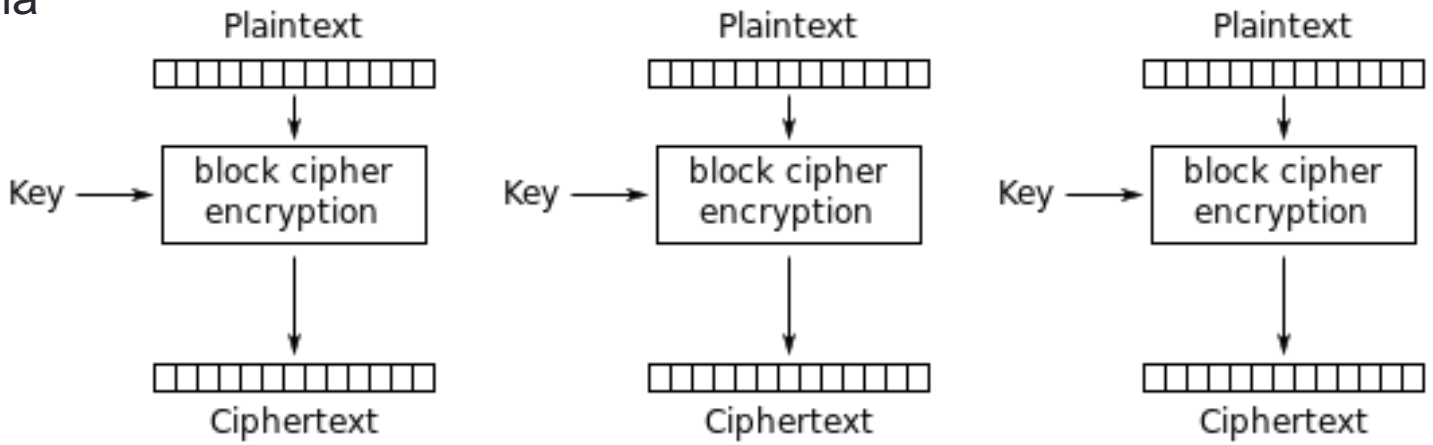
- 平文Mをn bitsの塊ごとに暗号化するもの
- 鍵Kの長さをk bitsとして、C=f(M,K)となるような関数で表現できる　Cもn bits
- kの大きさによって計算量的な安全性を保つ
- 現在主流の暗号化手法
  - DES、AESなど



Block Cipherの暗号利用モード（mode of operation)

- ECB(Electronic CodeBook)

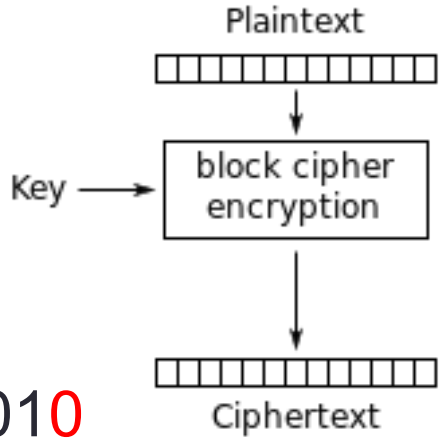
From Wikipedia



Electronic Codebook (ECB) mode encryption

平文が同じなら暗号文も同じになってしまう！

ECBモード

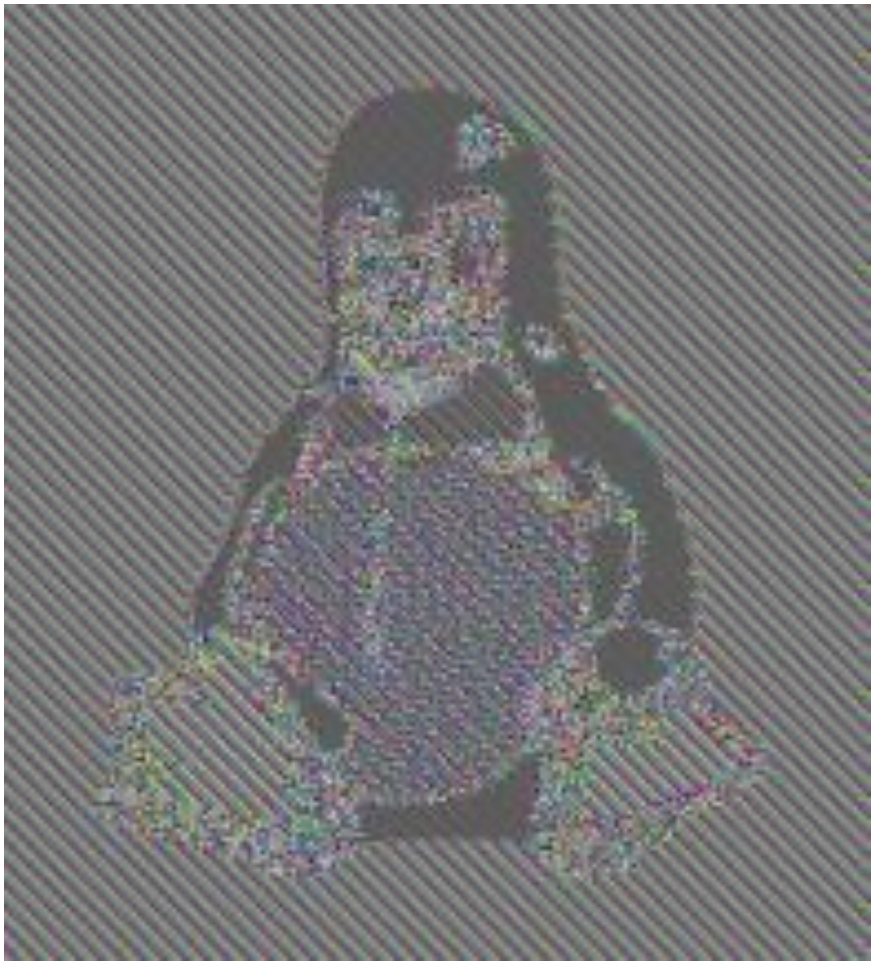


- 平文 m=101100010100101
- ブロック化
  m1 = 1011, m2 = 0001, m3 = 0100, m4 = 1010
- 鍵をπ = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ とする（転置）
- ブロック暗号文
  c1 = 0111, c2 = 0010, c3 = 1000, m4 = 0101
- 暗号文 c = 0111001010000101が得られる

例題：平文 m = 100110110110101111111 を暗号化せよ
ただし、鍵はπ = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ とする

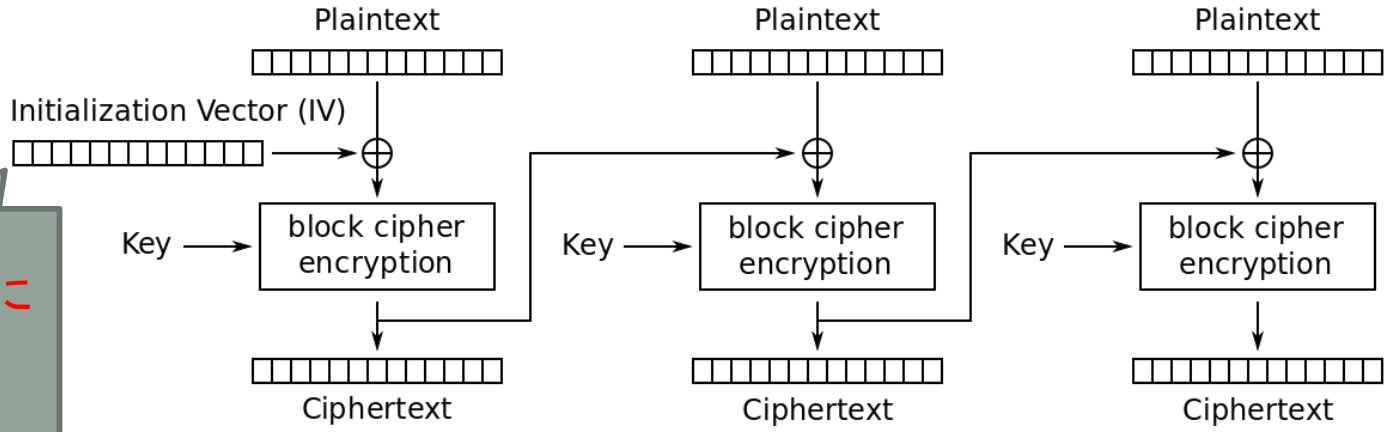
ECBの例

From
Wikipedia

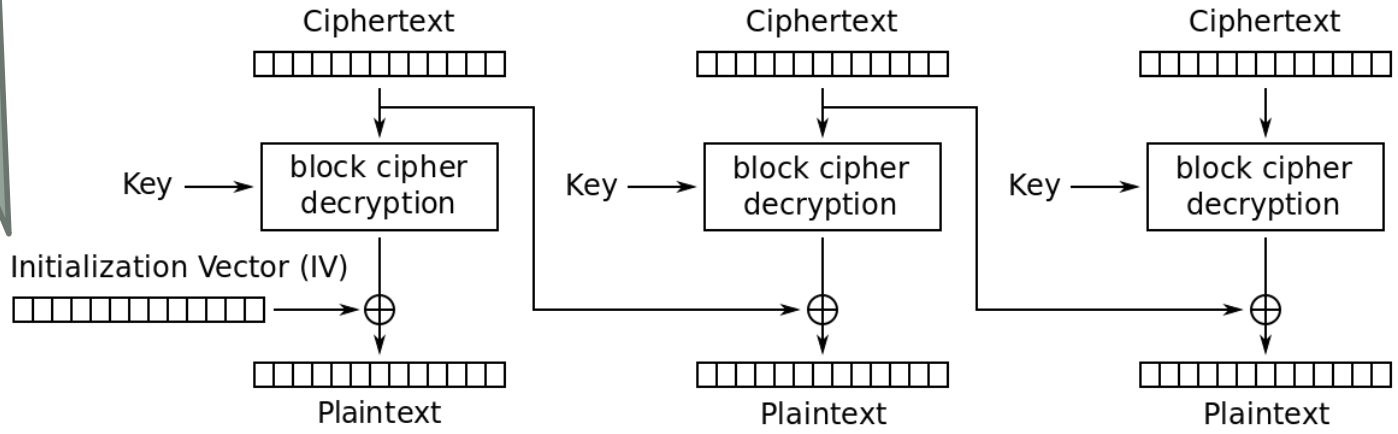


暗号利用モード：CBC（Cipher Block Chaining）

暗号化・復号に
鍵(Key)に
加えて
IVが必要

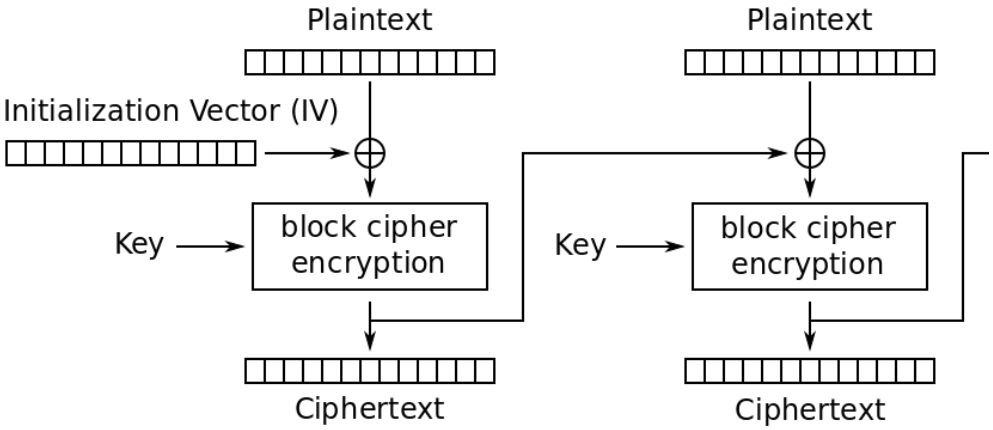


Cipher Block Chaining (CBC) mode encryption



Cipher Block Chaining (CBC) mode decryption

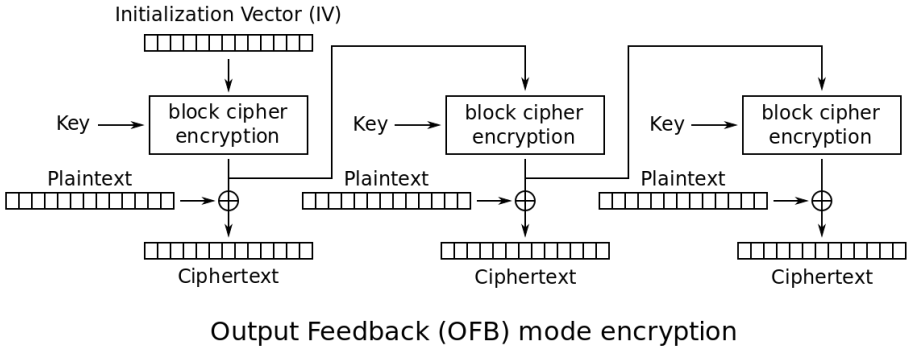
CBCモード



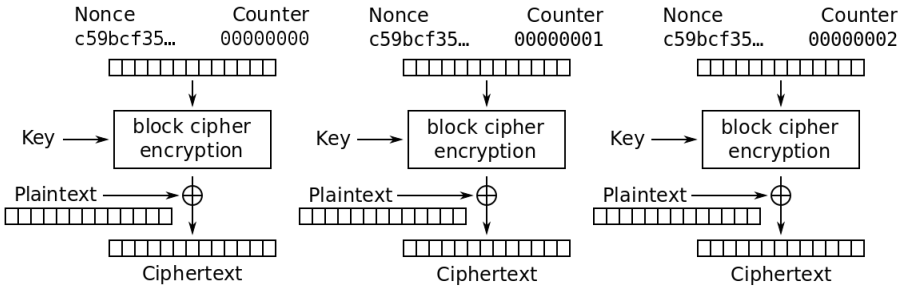
- 平文 m=101100010100101
- ブロック化
  m1 = 1011, m2 = 0001, m3 = 0100, m4 = 1010
- 鍵をπ = $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ とする（転置）、初期ベクトルIV（c0）=1010とする
- ブロック暗号文 ex. c1 = Eπ(c0⊕m1)
  c0 = 1010, c1 = 0010, c2 =0110, c3 =0100, c4 =1101
- 暗号文 c = 0010011001001101が得られる

例題：暗号文c = 0010011001001101を復号化せよ

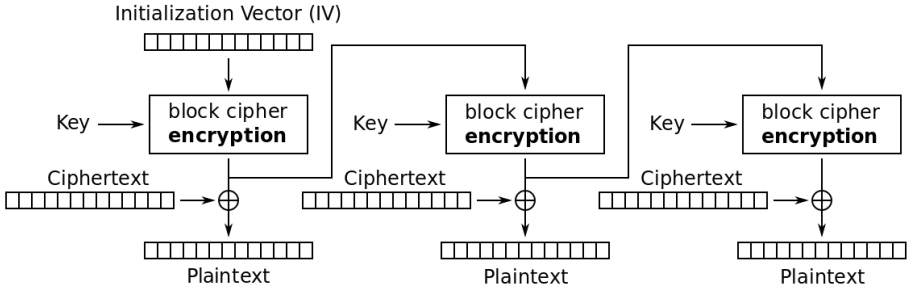
Block暗号を用いたStream暗号



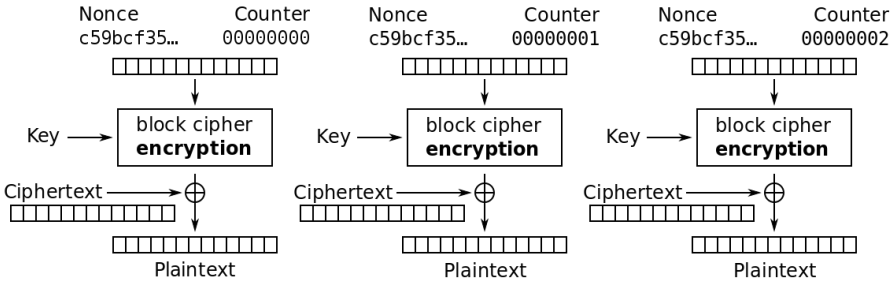
Output Feedback (OFB) mode encryption



Counter (CTR) mode encryption



Output Feedback (OFB) mode decryption



Counter (CTR) mode decryption

Output Feedback (OFB) mode

Counter (CTR) mode