リモートアクセス

- リモートアクセス
- 暗号化
- 公開鍵暗号方式
- 公開鍵暗号方式によるユーザ認証

リモートアクセス

ネットワークを経由して離れた場所にあるコンピュータに接続する

- ウェブ
- メール

- スーパーコンピュータ
  - 富岳@神戸

- 観測
  - 遠隔地にある観測装置を操作

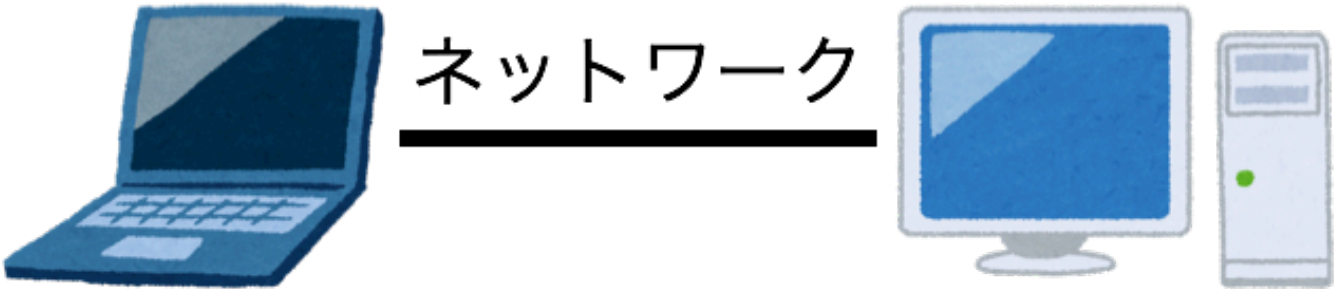
地球科学科サーバ earth

ホスト名　　earth.desc.okayama-u.ac.jp
IP アドレス　150.46.242.61

- 学科ホームページ
- 学科メーリングリスト

リモート・ログイン

こっちにあるパソコンを使って，ネットワーク経由で，
あっちにある計算機にログインする



- 計算機にログインするためには，ユーザ認証に必要な情報をネットワーク経由で送る必要がある
- ネットワーク上を流れるデータは丸見え
- 暗号化は必須

画像：いらすとや

盗聴を防ぐための暗号化

ネットワーク上を流れるデータは丸見えであるという前提で，見られてはいけないものは暗号化して流す

暗号とは

- 見せたい相手にだけ情報が伝わる
- それ以外の相手には情報が読めない

暗号化　平文 (元データ) を暗号文に変換すること
復号　暗号文を平文に戻すこと

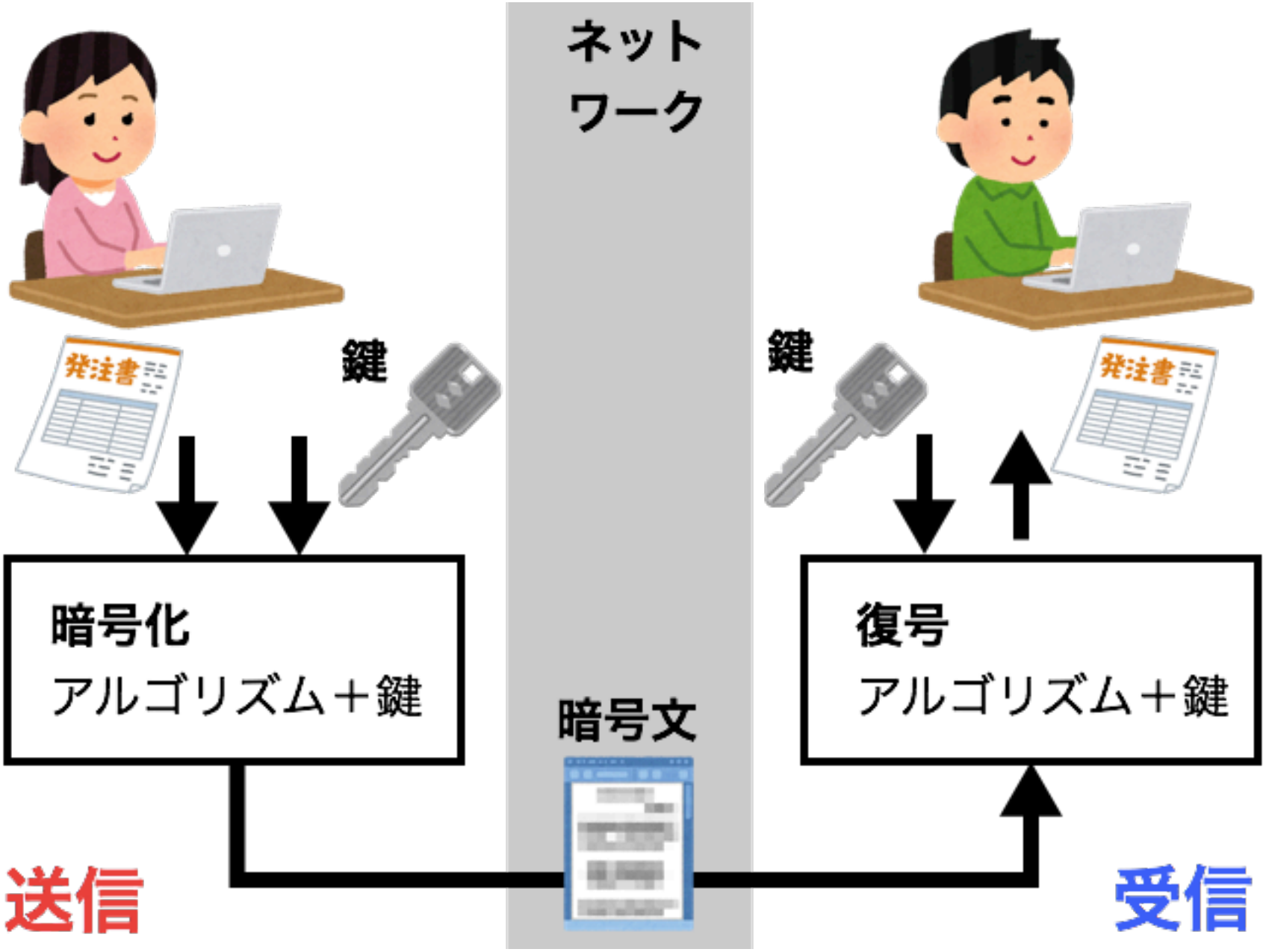
暗号の例：シーザー暗号

暗号化アルゴリズム

- アルファベットを n 文字だけ後ろにずらす
- 鍵＝ずらす文字数 n

鍵	暗号文	平文	
3	dwqrvskhuh	atmosphere	
-1	HAL	IBM	『2001 年宇宙の旅』
-1	Jdqnqn Ftmrn	?????? ?????	復号できましたか？

暗号化通信の例



鍵配送問題

暗号を使った通信をおこなうための鍵をどのようにして相手に届けるか，という問題

- 鍵を配送するのにネットワークは使えない
- 鍵を暗号化して送ることにすると，暗号化された鍵を復号するための鍵が必要となり...

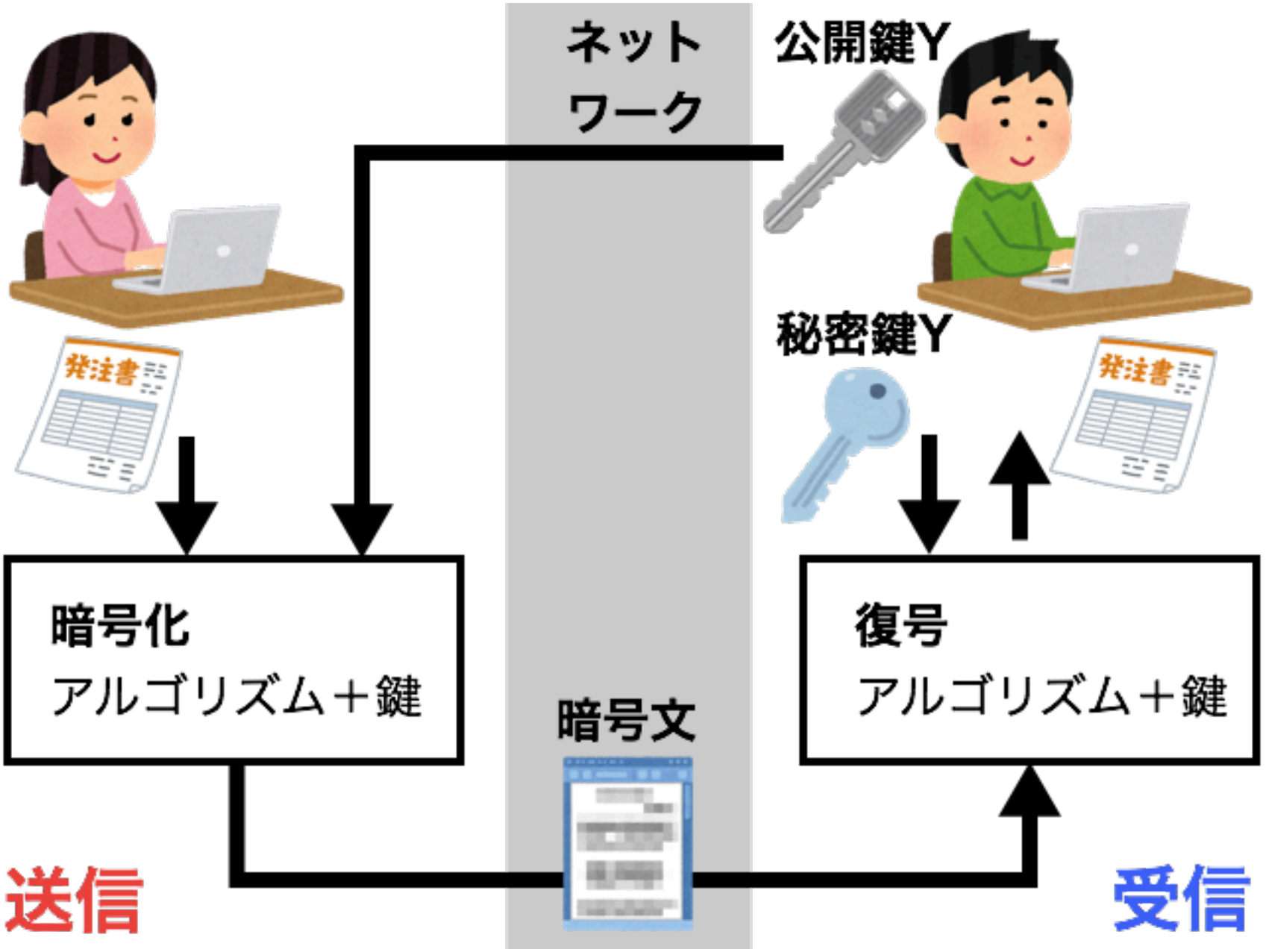
公開鍵暗号方式

公開鍵と秘密鍵のペアで鍵としてはたらく

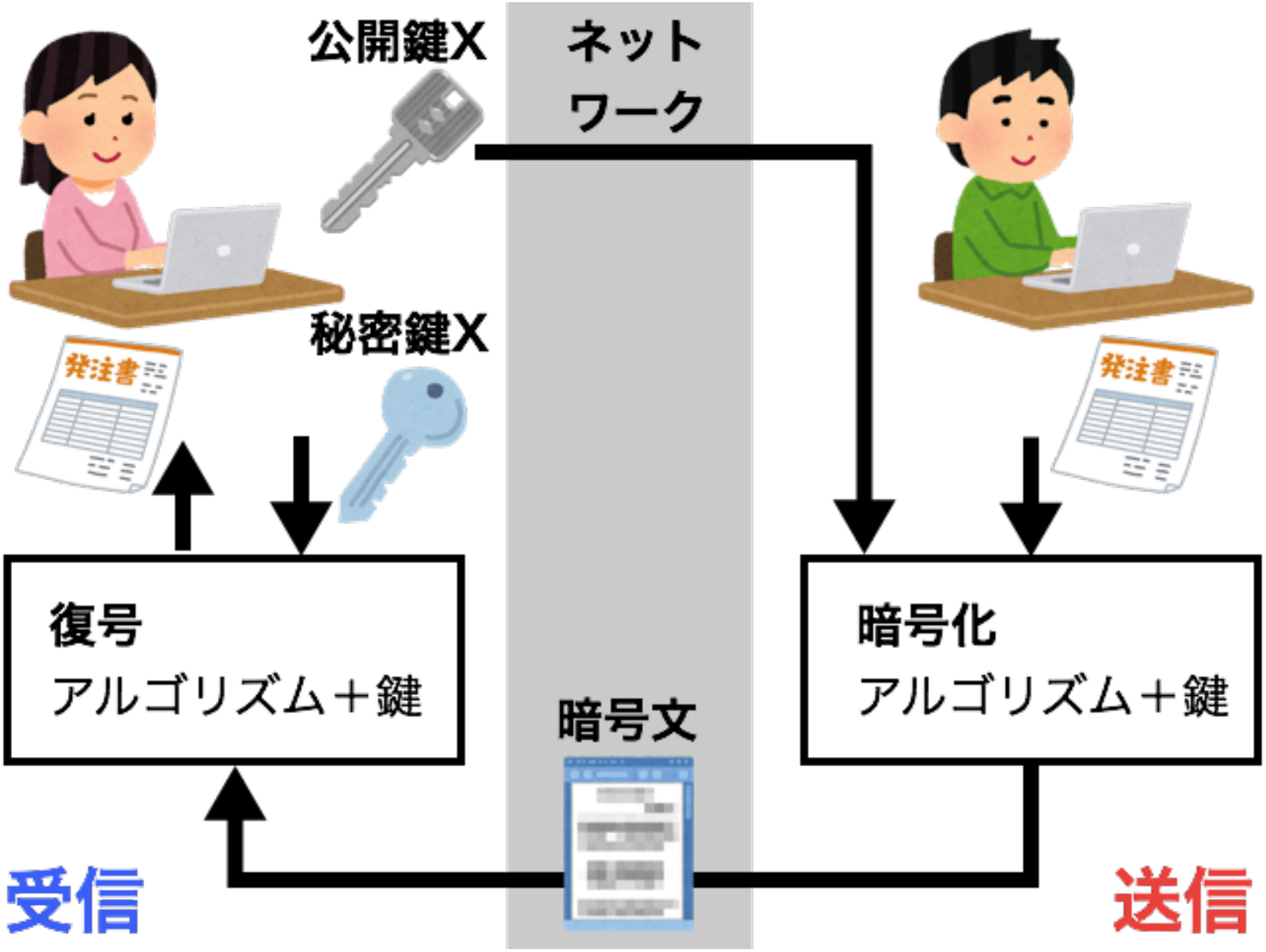
- 公開鍵で暗号化されたものは，
  ペアの秘密鍵でのみ復号できる
- 秘密鍵で暗号化されたものは，
  ペアの公開鍵でのみ復号できる

暗号化のアルゴリズムと暗号化に使われた鍵 (公開鍵) を知っていても，それだけでは復号できない

公開鍵暗号方式を使った通信



公開鍵暗号方式を使った通信



公開鍵暗号方式の特徴

利点　鍵の配布が簡単

- 公開鍵 (public key) はネットワーク上で公開する
- 秘密鍵 (private key) はネットワーク上を流れない
- 不特定多数の相手と暗号化通信できる
  - 通信相手の公開鍵をとってくるだけ

欠点

- 共通鍵暗号に比べて処理に時間がかかる

公開鍵暗号方式によるユーザ認証

鍵を使ってユーザ認証する (パスワードは使わない)

- あらかじめ接続先のサーバに自分の公開鍵を登録
- サーバは，相手が登録された公開鍵に対応する秘密鍵を持っているかどうかで，ユーザ認証する

公開鍵暗号方式によるユーザ認証

1. ユーザは，共通鍵を作成し，接続先サーバの公開鍵で暗号化して，接続先サーバに送る
2. サーバは，送られてきた共通鍵をサーバの秘密鍵で復号する
3. サーバは，ランダムな値を生成し，ユーザが登録した公開鍵を使って暗号化し，ユーザに送る
4. ユーザは，送られてきたデータを自分の秘密鍵で復号し，先に送った共通鍵で暗号化して，サーバに送る
5. サーバは，ユーザから返送されたデータを共通鍵で復号し，返送された値が正しければ，ユーザを本物と認証する

まとめ

パスワード認証と公開鍵認証

- パスワード認証　ユーザ ID とパスワード
- 公開鍵認証　ユーザ ID と秘密鍵 (と公開鍵)

秘密鍵

- 他人に見せてはいけない (盗まれてはいけない)
- 秘密鍵はパスフレーズで守る
  - 秘密鍵を使うときにパスフレーズを訊かれる

公開鍵

- 他人に見せてよい
- 接続先のホストに登録して公開鍵認証を使う

小悪魔女子大生のサーバエンジニア日記

aico (著)
株式会社ディレクターズ (著)
村井 純 (監修)

Kryptos

Photo: Jim Sanborn (CC BY-SA 3.0)

CIA 本部に設置されている彫刻　1990 年 11 月 3 日 設置

- ４つのメッセージ，うち３つ解読，１つ未解読