ネットワーク・コンピューティングと暗号化

公開鍵暗号を使ったリモートアクセスのための基礎知識

はしもとじょーじ

ネットワーク・コンピューティング

こっちにいながらにして、あっちにある計算機を使う

- 多数で共有する計算機の利用
  - 大型計算機
  - 地球科学科サーバ earth
- 共同研究
  - データの転送
- お出かけ中のメール確認
- etc

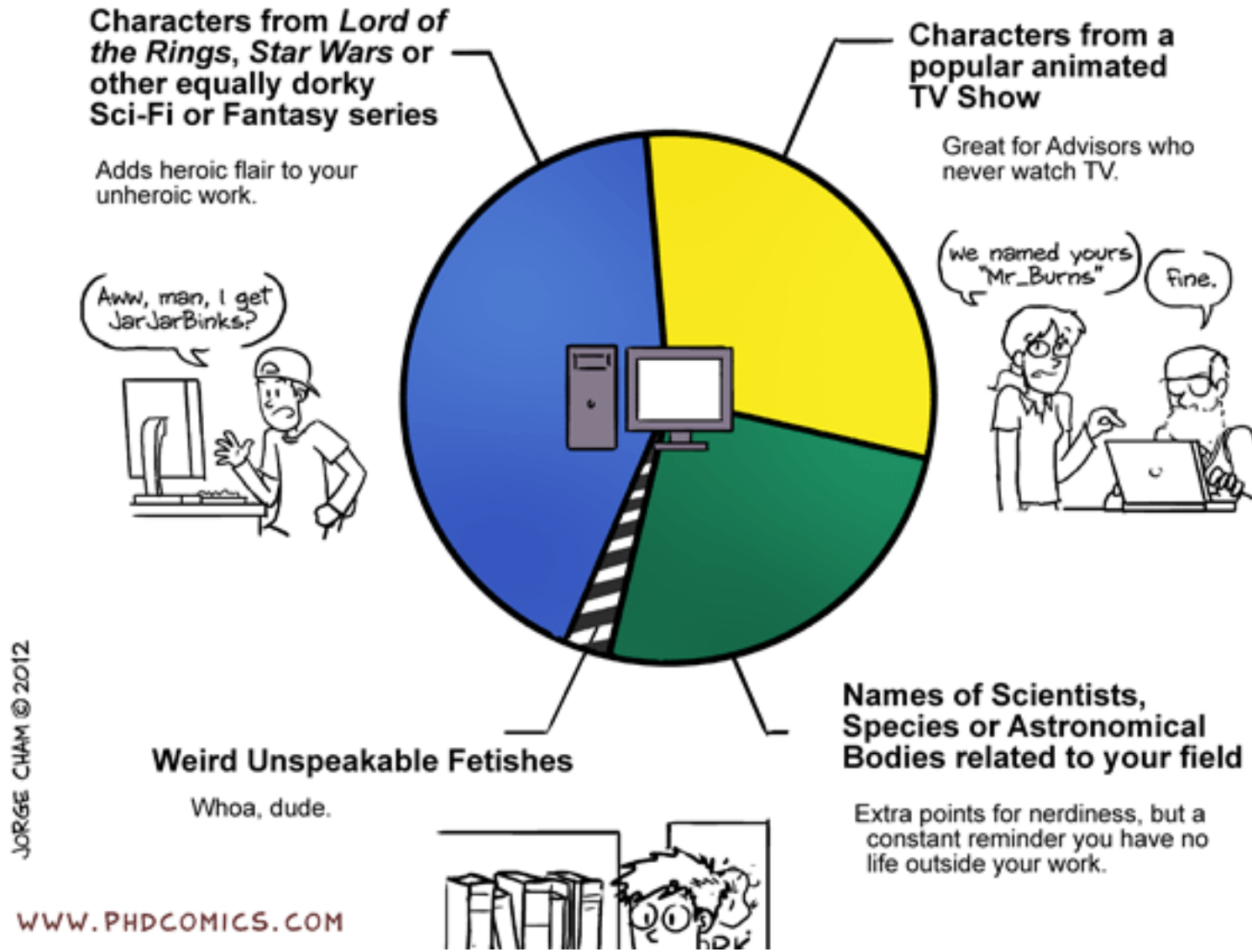
地球科学科サーバ earth

earth.desc.okayama-u.ac.jp

IP アドレス　　150.46.242.61

- ウェブサーバ
  学科ホームページ
- メールサーバ
  学科のメーリング
  リストの運用

MOST POPULAR THEMES FOR NAMING YOUR LAB/OFFICE COMPUTERS



http://www.phdcomics.com/comics/archive.php?comicid=1468

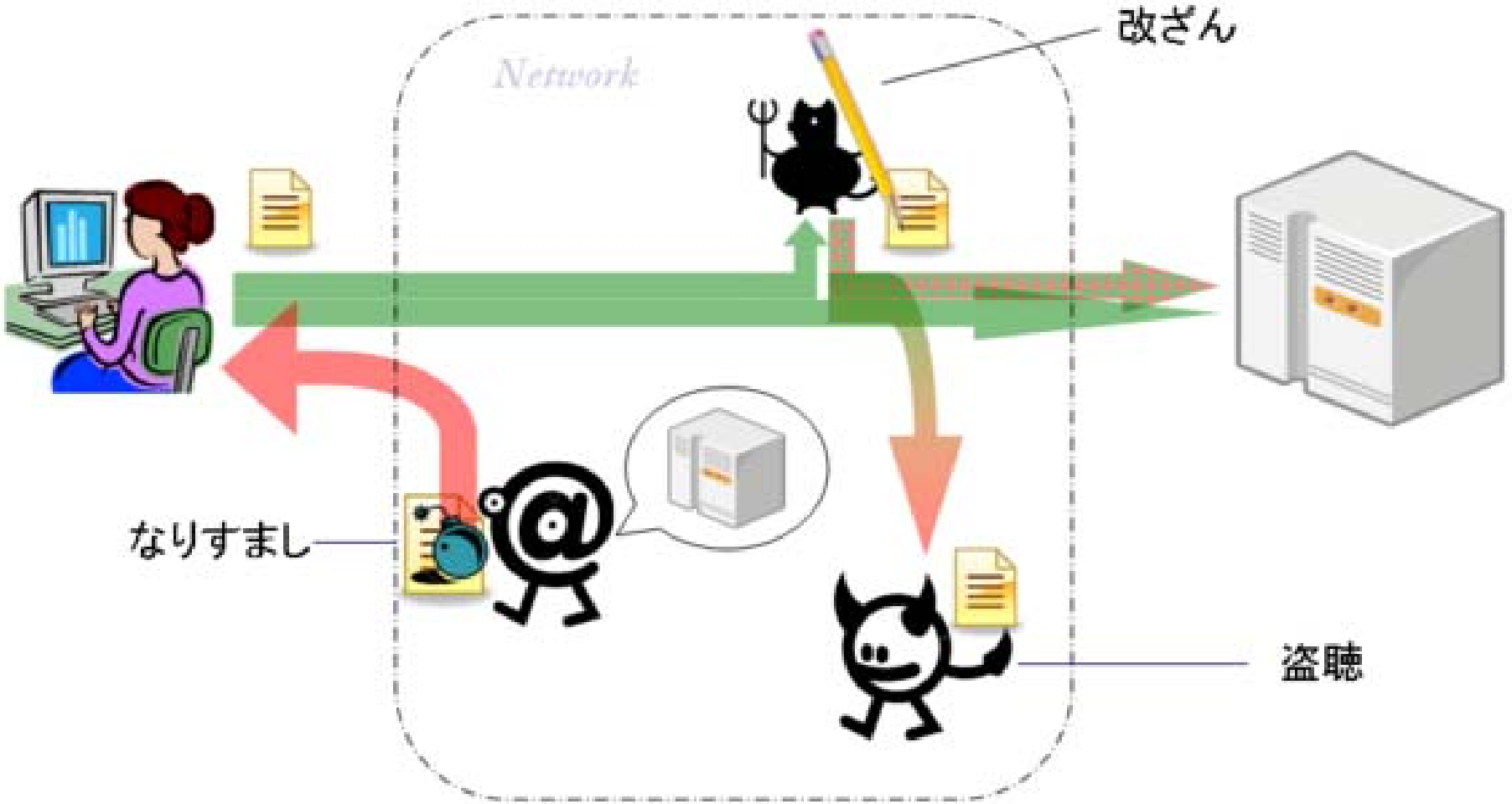
リモート・ログイン

こっちのパソコンを使ってネットワークを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、ユーザ認証の手続きが必要

ユーザ認証に必要な情報をネットワーク経由で送ってやる必要がある　→ 暗号化が必要

ネットワークに潜む脅威



脅威は，大きくわけて 3 種類

盗聴を防ぐための暗号化

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

暗号化と復号

- 元データ(平文)を暗号文に変換すること
- 暗号文を平文に戻す手続きを復号という

復号の方法を知らなければ、暗号文を入手しても元データを復元できない

暗号の例：シーザー暗号

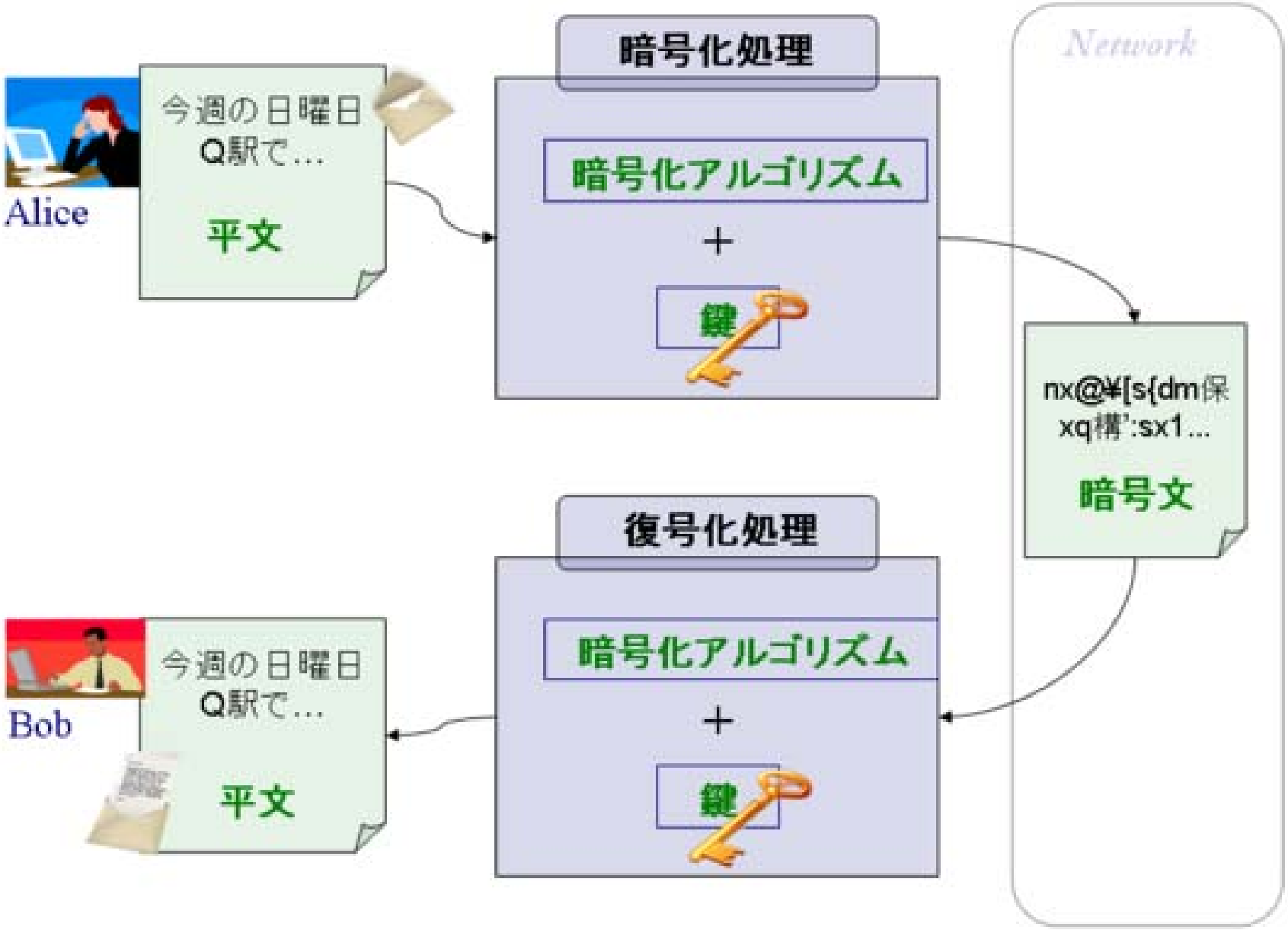
アルファベットを n 文字だけ後ろにずらす

- IBM → HAL (n=−1)
- atmosphere → dwprvskhuh (n=3)
- ?????? → jdqnqn (n=−1)

暗号化アルゴリズム

- この例では n 文字だけ後ろにずらす操作
- この n は任意に選ぶことができる
- ずらす文字数＝鍵

暗号化通信の例


Alice
今週の日曜日
Q駅で…
平文
暗号化処理
暗号化アルゴリズム
＋
鍵
Network
nx@¥[s{dm保
xq構':sx1…
暗号文
復号化処理
暗号化アルゴリズム
＋
鍵
Bob
今週の日曜日
Q駅で…
平文

共通鍵暗号方式と公開鍵暗号方式

共通鍵暗号方式

暗号化と復号に同じ鍵を使う
処理にかかるコストが比較的に小さい

公開鍵暗号方式

公開鍵と秘密鍵の２種類の鍵をペアで使う
処理にかかるコストが比較的に大きい

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

- ネットワークを使って鍵を安全に届けるためには，暗号化する必要がある
- 暗号化された鍵を復号するためには鍵が必要

公開鍵暗号方式

秘密鍵と公開鍵のペアで鍵として働く

- 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、
  ペアの公開鍵で復号できる

暗号化に使われた鍵(公開鍵)を知っていても、
秘密鍵を知らなければ復号できない

公開鍵暗号方式を使った通信

太郎(送信者)		花子(受信者)
	←	花子の公開鍵を送る
花子の公開鍵で文書を暗号化する		
暗号文を送る	→	
		花子の秘密鍵で暗号文を復号する

公開鍵暗号方式の特徴

メリット　鍵の配付が簡単

- 公開鍵(public key)はネットワーク上で公開すればよい
- 秘密鍵(private key)が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

デメリット

- 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ー認証

パスワードではなく，鍵を使ってユーザー認証をおこなう

[0] あらかじめ earth に自分の公開鍵を登録

最初に共通鍵を交換する

[1] ユーザーは共通鍵を作成する
earth の公開鍵で暗号化して earth に送る

[2] earth は送られてきた共通鍵を自分(earth)の秘密鍵で復号する

ユーザー認証

[3] earth はランダムな値を作る
あらかじめ登録されているユーザーの公開鍵によって暗号化してユーザーに送る

[4] ユーザーは自分の秘密鍵で復号する
先に送った共通鍵で暗号化して earth に送り返す

[5] earth はユーザーから返送された値が正しければ，ユーザーを本物と認証する

今日の作業

1．公開鍵と秘密鍵のペアを作成する
   - ssh-keygen

2．earth にアカウントを申請する
   - gate-toroku-system
   - 公開鍵を登録する

3．earth にログインしてみる

参考文献

小悪魔女子大生の
サーバエンジニア日記

技術評論社

http://www.amazon.co.jp/dp/477414522X/