暗号技術入門

鈴木鐵也 (@szktty)

2011/6/18

アジェンダ

- 現在の主な暗号技術を紹介
- 実際にどう使われているかを中心にストーリー仕立てで紹介
- 数学的な理論には深入りしません

お前、誰よ

- フリーランスで、今は某ベンダで雑用してます
- ネットワークプロトコルの調査をすることも多く、 暗号の話題に触れる機会が多いです

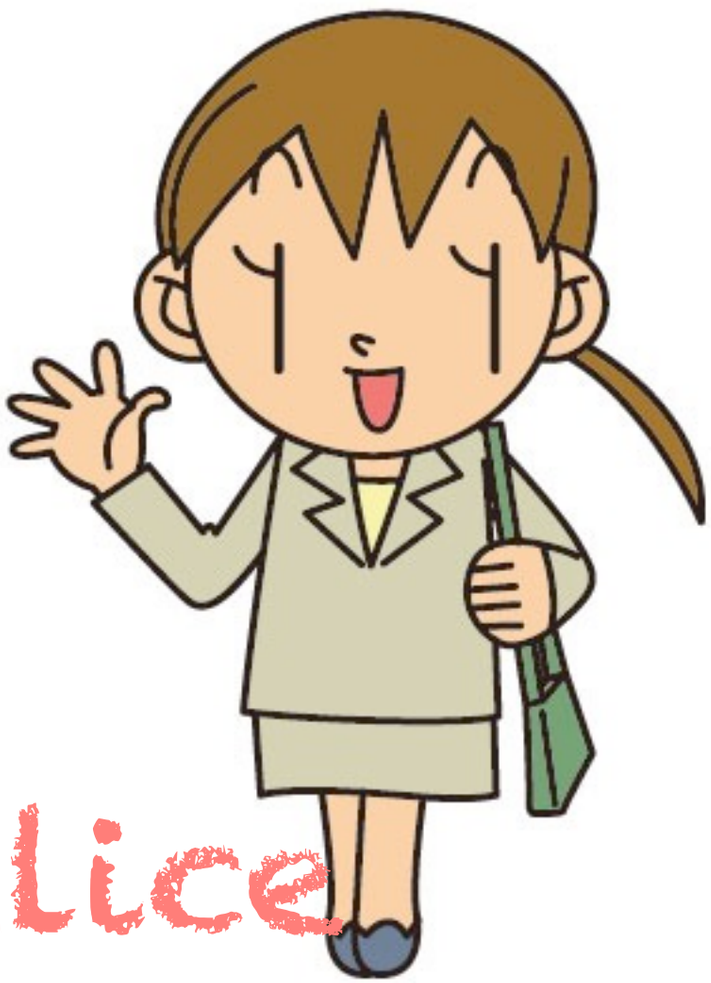
はじめまーす

暗号サスペンス劇場

ストーカー：逃げ切れぬ愛

昔々、あるところに
ボブとアリスとマロリー
がいました。

Bob



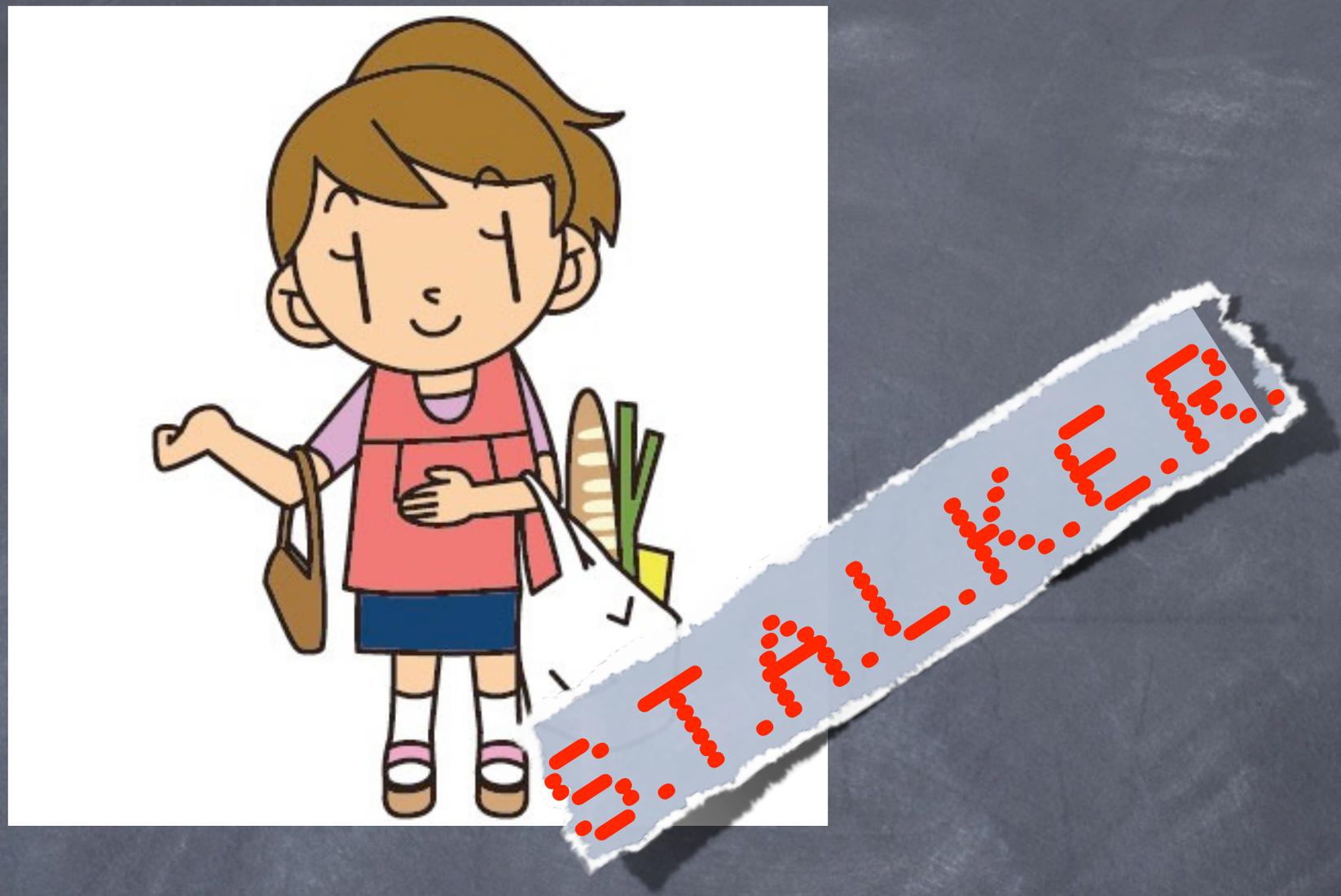
Alice

ボブはアリスと

職場恋愛中。

でもみんなには内緒。

だって…



マロリーがストーカー。

ばれたらやばい。

ボブ「そうだ、メールで
プロポーズしよう」

ボブのイメージ：

ボブ：”Would you marry me?”
（結婚して！）

アリス：”Absolutely!”
（もちろんよ！）

3つの問題点 (1)

1. マロリーによる盗聴

2. マロリーによる捏造

3. マロリーによるなりすまし

1. マロリーによる盗聴

もしメールを見られたら...


BANG!!

マロリーに見られても
中身がわからなければいい
（機密性）

3つの問題点 (2)

1. マロリーによる盗聴

2. マロリーによる捏造

3. マロリーによるなりすまし

2. マロリーによる捏造

ペンは銃より強し

マロリーが
捏造しちゃうかも？

アリス：”Absolutely!”
（もちろんよ！）

↓

アリス：”Absolutely NOT!”
（絶対にイヤ！）

マロリーの捏造の証拠が
残るようにすればいい
（正真性、完全性）

3つの問題点 (3)

1. マロリーによる盗聴

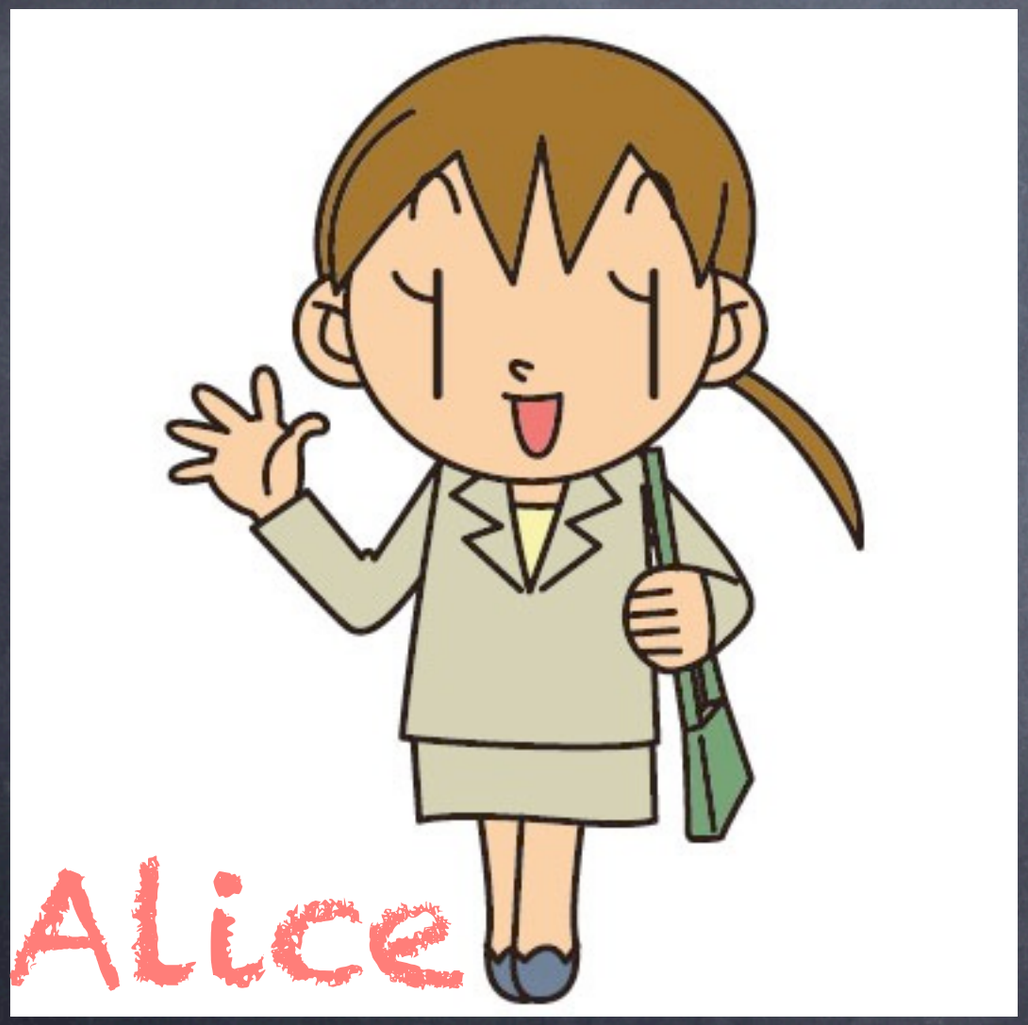
2. マロリーによる捏造

3. マロリーによるなりすまし

3. マロリーによるなりすまし

別れさせ屋だけど質問ある？

ボブ？：”Let’s break up…”
（別れよう…）



本当にボブからの
メール？

メール送信者が
ボブだと証明できればいい
（認証）

ITサスペンス劇場

ストーカー：逃げ切れ受

解決編

3つの問題点 (1)

1. マロリーによる盗聴

2. マロリーによる捏造

3. マロリーによるなりすまし

メールを暗号化する

- 内容がわからなくなる
- 共通鍵暗号（対称暗号）を使う
- 公開鍵暗号でも可、しかし遅い
- どちらにしろ鍵が必要

共通鍵暗号？

- 暗号化に使った鍵で復号化する
  「共通鍵はいつもひとつ！」
- ボブとアリスが同じ鍵を共有する必要がある
- 鍵がマロリーにばれたらおしまい

「結婚しよう！」

平文（ひらぶん）

暗号文

人が読んでも意味ないデータ

3つの問題点 (2)

1. マロリーによる盗聴

2. マロリーによる捏造

3. マロリーによるなりすまし

メールを要約する

- メールの内容を数十バイトに縮める
  - 一文字でも変更するとすべて変わる
  - メッセージダイジェストと呼ぶ
- 一方向ハッシュ関数を使う

寿限無、寿限無 五劫の擦り切れ 海砂利水魚の 水行末
雲来末 風来末 食う寝る処に住む処 やぶら小路の藪柑子
パイポパイポ パイポのシューリンガン シューリンガンの
グーリンダイ グーリンダイのポンポコピーの
ポンポコナーの 長久命の長助

一方向ハッシュ関数

ダイジェスト

くぁwせdrftgyふじこlp

え？暗号化に似てない？

- ダイジェストから元の文は復元できない
- どんな大きいデータでも、
  ダイジェストは数十バイトに納まる
- 鍵がいらない

暗号化だけじゃだめ？

- 復号化したメールが、ボブが送った
  元のメールと一致するとは限らない
- 元のメールのダイジェストと
  復号化したメールのダイジェストを比較
  - 一致すれば OK

3つの問題点 (3)

1. マロリーによる盗聴
2. マロリーによる捏造
3. マロリーによるなりすまし

鍵つきダイジェスト

- 誰でも（マロリーでも）
  同じダイジェストを作れちゃう
- ボブとアリスしか知らない情報
  （＝鍵）でダイジェストを計算する
- このアルゴリズムをHMACと呼ぶ

組み合わせてみよう！

平文

共有

共通鍵
HMAC鍵

共通鍵暗号

一方向
ハッシュ関数
＋
HMAC

共有

暗号文 ＋ ダイジェスト

最終的に送信するデータ

暗号文 + ダイジェスト

まだ足りない！

足りないもの？

暗号文 ＋ ダイジェスト

本当にボブからのメール？

ネ？

事件の鍵は鍵にあり？

ボブとアリスは二つの鍵を共有している

↓

ボブもアリスも
同じ「暗号文+ダイジェスト」を作れる

↓

ボブもアリスも自作自演できる

事件の鍵は鍵にあり？

↓

友達にプロポーズを証明できない

（第三者への証明）

↓

もし自作自演でも逃げ切れる

（否認防止）

長くなったので

続きはWebで！

ウソです。

次回あったらやるかも

キーワードは
デジタル署名と
公開鍵暗号です

Thank you!