University
of Ljubljana

Faculty
of civil and geodetic engineering

Computer Mediated Communication (CE6014)

Secure Communication

November 2011

Matevž Dolenc
University of Ljubljana

Content

- Fundamental security concepts
  - Introduction to cryptography
  - Public-key cryptography, Certificates and Certificate Authorities (CA)
- Security problems/questions
  - Delegation and single sign-on (SSO)
  - Cloud computing security/trust/availability

What is a Secure Communication

- The tree pillars of a secure communication
  - *Privacy*. A secure conversation should be private – only the sender and the receiver should be able to understand the conversation. This is generally achieved by encryption/description algorithms.
  - *Integrity*. A secure conversation should ensure the integrity of the transmitted message – the receiver must know for sure that the message he is receiving is exactly the same that the transmitter sent.
  - *Authentication*. A secure conversation should ensure that the parties involved in the communication are who they claim to be.

What is a Secure Communication

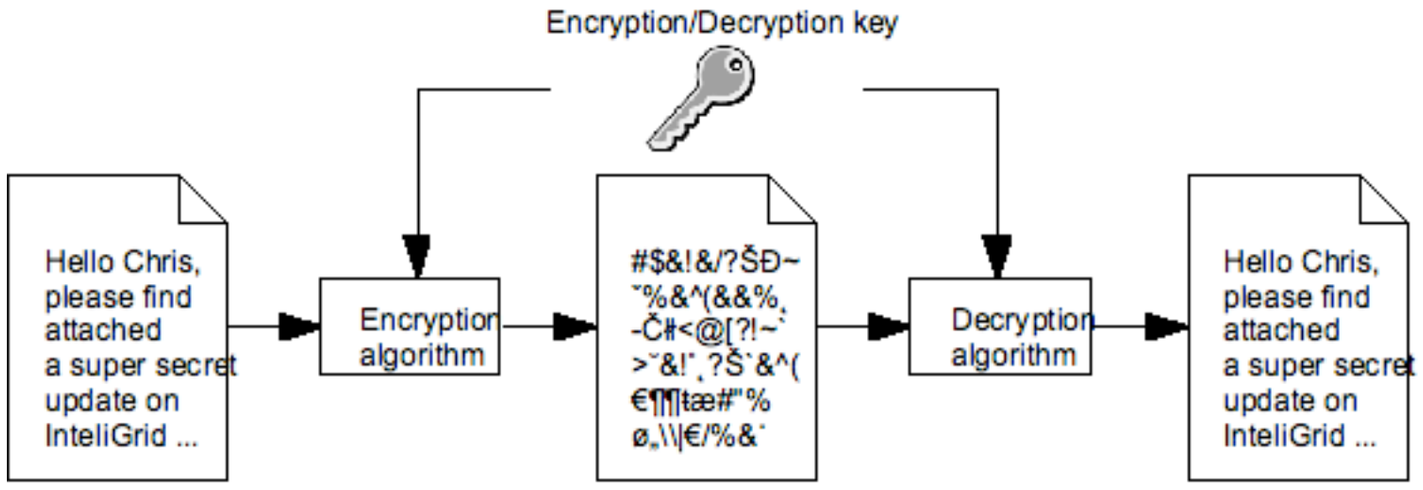
- Closely related to the tree pillars
  - *Authorisation*. a mechanisms that decide when a user is authorised to perform a certain task; ... generally related to authentication.

Introduction to Cryptography

- Cryptography - the art of writing in secret characters
  - *Encrypting*. Translating "normal message" to a message written with "secret characters" (encrypted message)
  - *Decrypting*. Translating a message written with "secret characters" into readable message (unencrypted message)
  - One of the most important areas in comp. security – provides underlying technology for the tree pillars of secure communication

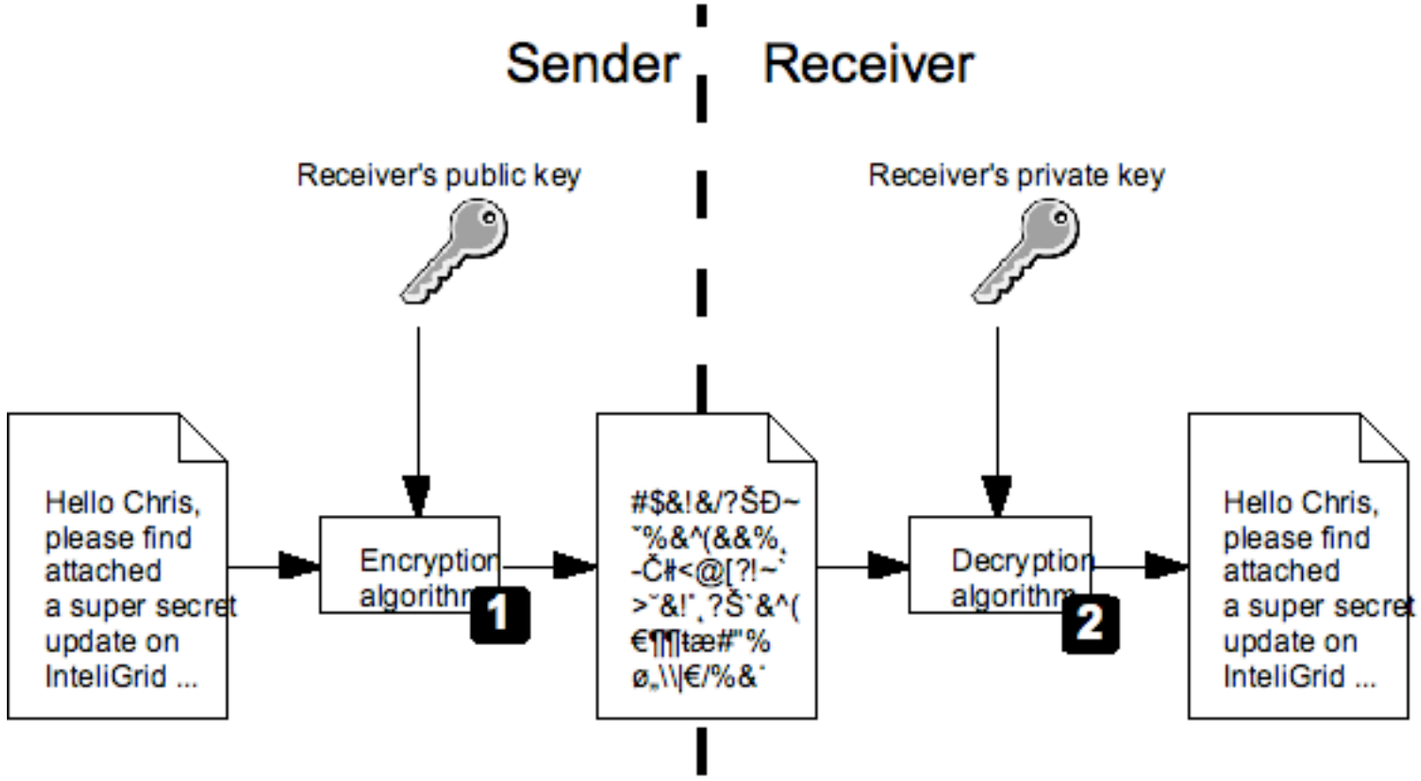
Introduction to Cryptography

- Key-based algorithms
  - Symmetric

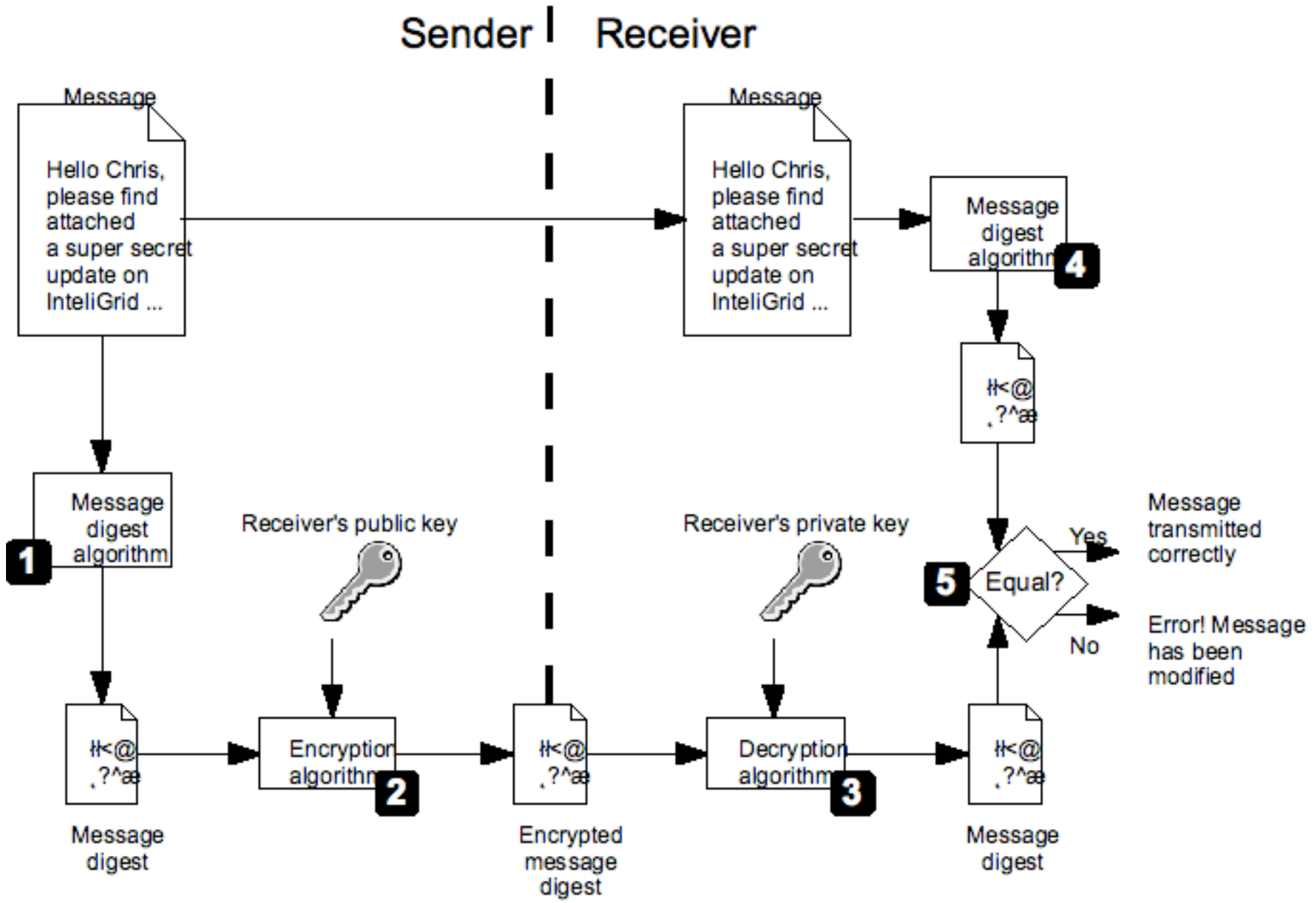


Introduction to Cryptography

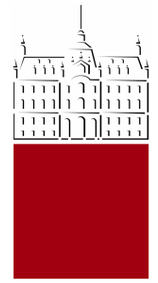
- Key-based algorithms
  - Asymmetric



Digital Signatures



Certificates and Certificate Authorities (CA)



- Digital signatures
  - Digital signature only guarantee that whoever sent the message has a private key corresponding to the public key
  - How can we be sure that the sender is who he claims to be?

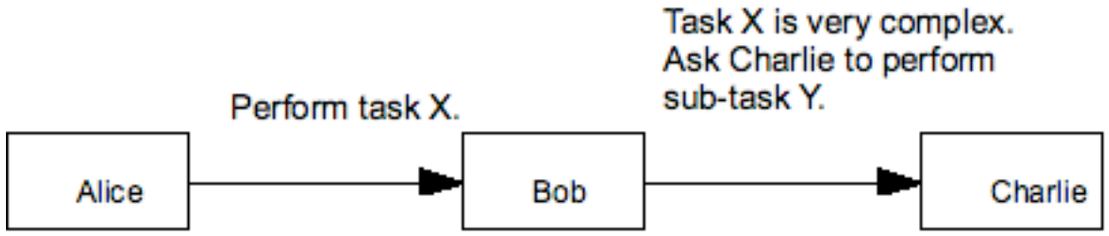
- Digital certificate ...
  - is digital document that certifies that a certain public key is owned by a particular user.
  - signed by a third party called certificate authority (CA)
  - support the third pillar of the secure conversation: authentication

Certificates and Certificate Authorities (CA)

- It is all about trust
  - trust the CA that signs the certificate
  - you must decide by yourself whether you trust or do not trust a CA; list of trusted CAs
- CA hierarchies
  - Trusted CA's list
  - Who signs the CA's certificate?
  - Self-signed certificate → root CA

Delegation

- The problem

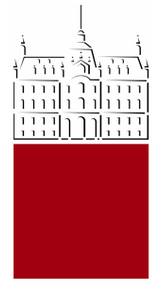


- The solutions: proxy certificates
  - Proxy certificate allows the holder of the certificate to act on behalf of the issuer of the proxy certificate.
  - Similar to X.509 digital certificates, but not signed by CA – they are signed by the end user
  - Limited time of validity

Single sign-on (SSO) 1/2

- Definition
  - Fantasy: One password for everything
  - Reality:
    - Most systems and applications already have their proprietary login functionality.
    - Reduce logins for discreet systems (corporate systems, shared intranet/web applications, web logon aggregators)
- Problem
  - Mushrooming passwords
  - “Sticky note” password cache
  - Unencrypted text files on laptops/smartphones/etc.

Single sign-on (SSO) 2/2



- Risks
  - Single point of failure
  - Stolen credentials via insecure implementations
- Solutions
  - Traditional single sign-on
  - Password synchronisation
  - Authentication platforms

Cloud computing security

- Security risks

1. Privileged user access.
2. Regulatory compliances.
3. Data location.
4. Data segregation.
5. Recovery.
6. Investigative support.
7. Long-term viability.

European Network and Information Security Agency (EINSA), Cloud Computing Risk Assessment
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

Cloud computing trust

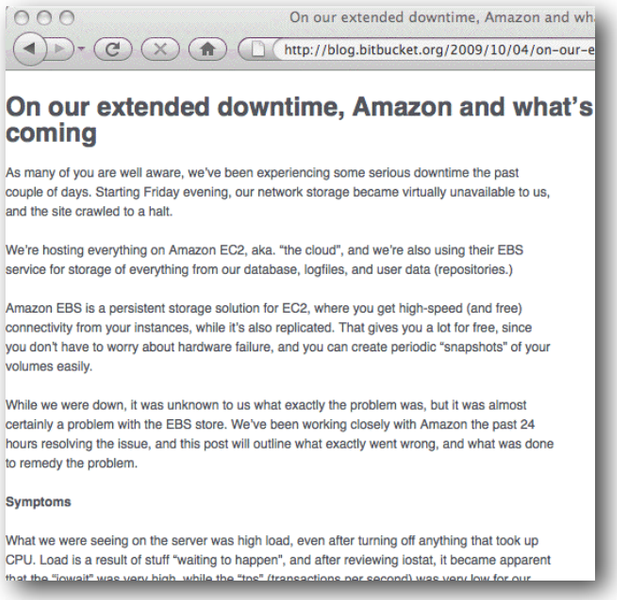
- Cloud computing is a form of outsourcing, and you need a high level of trust in the entities you'll be partnering with.
- It may seem daunting at first to realise that your application critically depend on the trustworthiness of your cloud providers, but this is not new:
  - network service provider
  - hardware and software vendors
  - service providers
  - data sources, etc.

Cloud computing availability 1/2

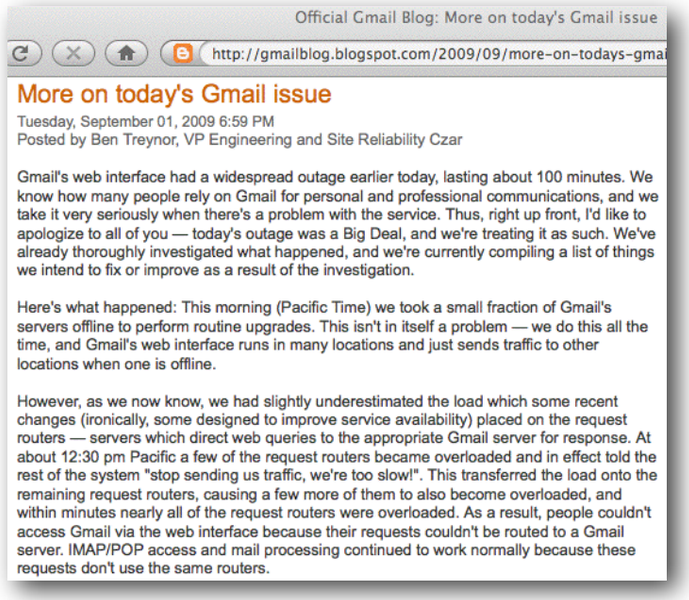
- Computer and network security is fundamentally about three goals/objectives:
  - confidentiality (C)
  - integrity (I), and
  - availability (A).
- Availability is the area where cloud based infrastructure appears to have had its largest (or at least most highly publicised) challenges to date.

Cloud computing availability 1/2

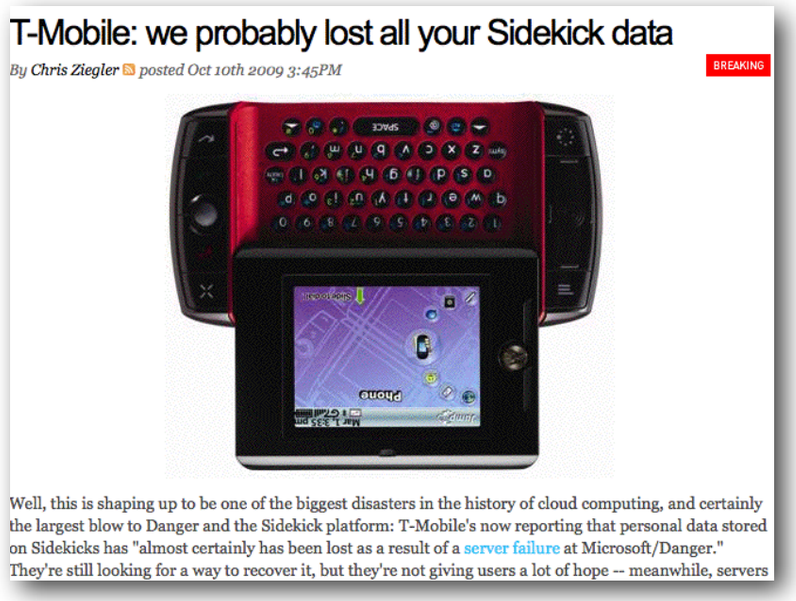
Bitbucket, DDOS'd off the air



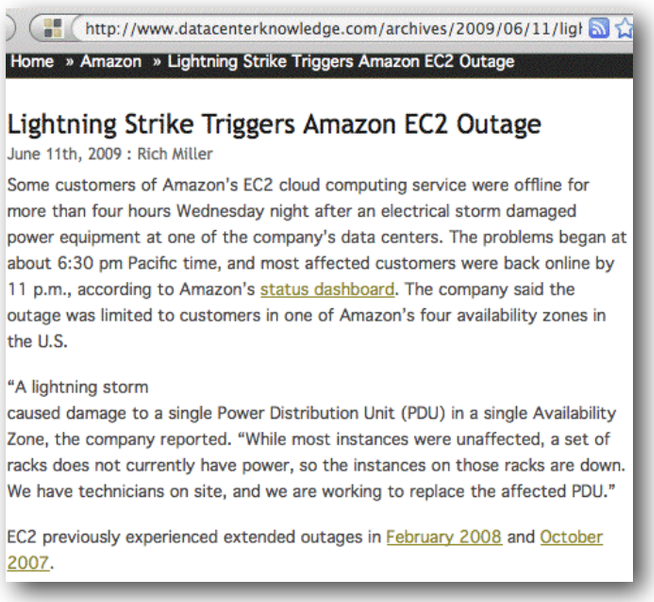
Maintenance induced cascading failures



Do Not Forget About the storage



And not forget about power issues



... and the most recent one

99.99 availability

=

52+ minutes downtime/year