System and Data Security

A CS Systems Prelim

Andy Sayler
04/16/14

How can we secure our systems and data in a robust, comprehensive, and easy-to-use manner?

Cryptography

Access Control

Data Storage

Usability & Management

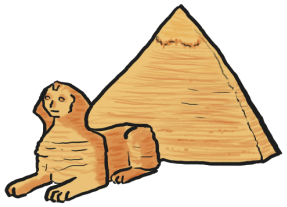
Diffie & Hellman - *New Directions in Cryptography* - 1976
Shamir, Adi - *How to Share a Secret* - 1979

Sandhu, et. al. - *Role-Based Access Control Models* - 1996
Bethencourt, et. al. - *Ciphertext-Policy A.B. Encryption* - 2007

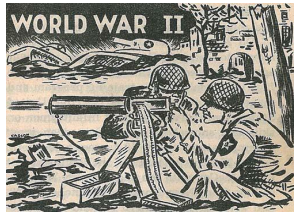
Mazières, et. al. - *Separating Key Mgmt from FS Security* - 1999
Kher & Kim - *Securing Distributed Storage* - 2005
Miltchev, et. al. - *Decentralized A.C. in Dist File Systems* - 2008

Samar, V. - *Unified Login with Pluggable Auth Modules* - 1996
Cox, et. al. - *Security in Plan 9* - 2002
Morgan, et. al. - *Federated Security: The Shibboleth Appr* - 2004

Cryptography



Classic “Crypto” (Substitution, Etc)



Kerckhoff’s Principle (1883)

Shannon Information Theory (1948)

Strong Symmetric Key Algorithms

D&H Asymmetric Crypto (1976)

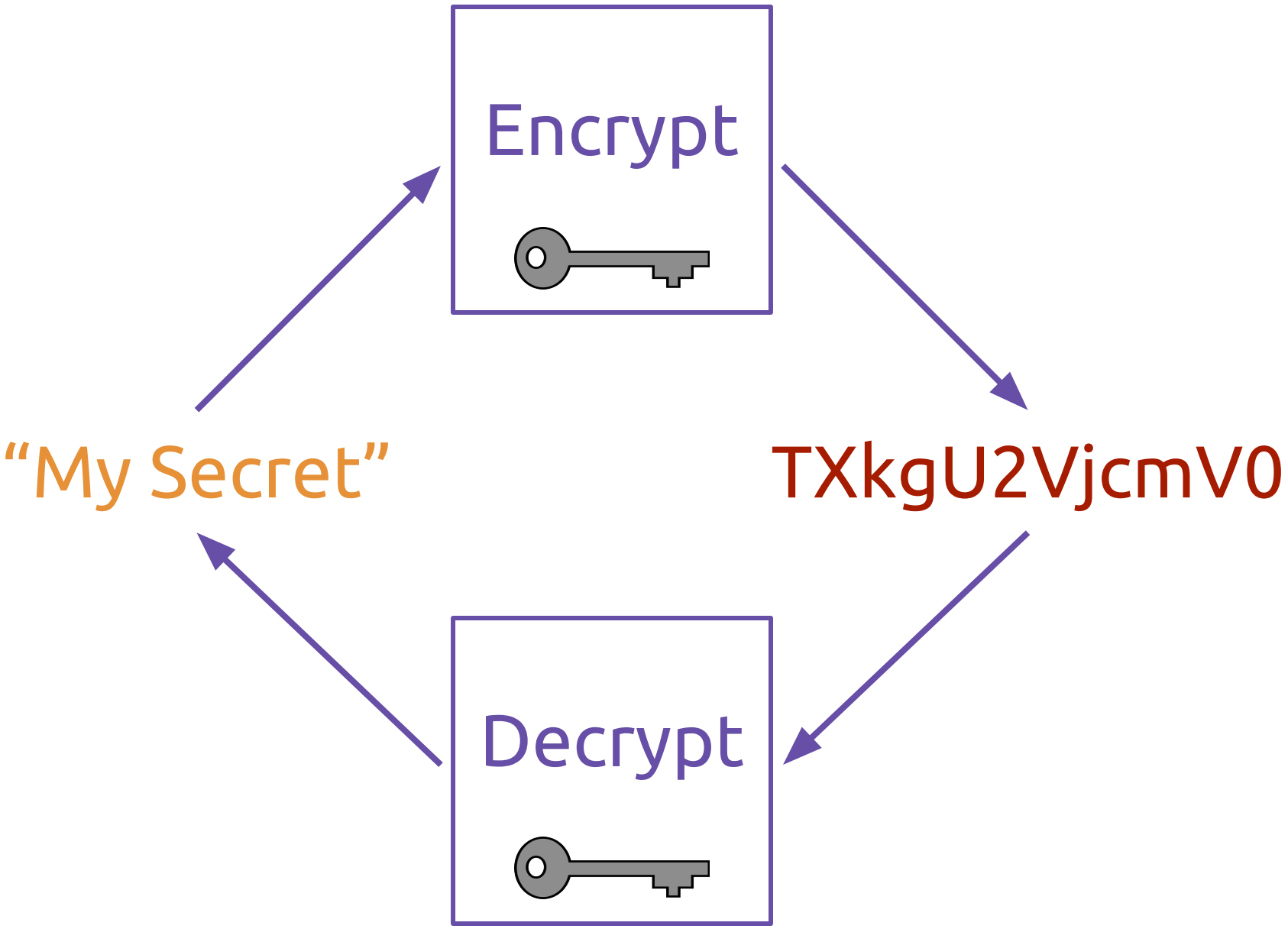
RSA Algorithm (1978)

Shamir Secret Sharing (1979)

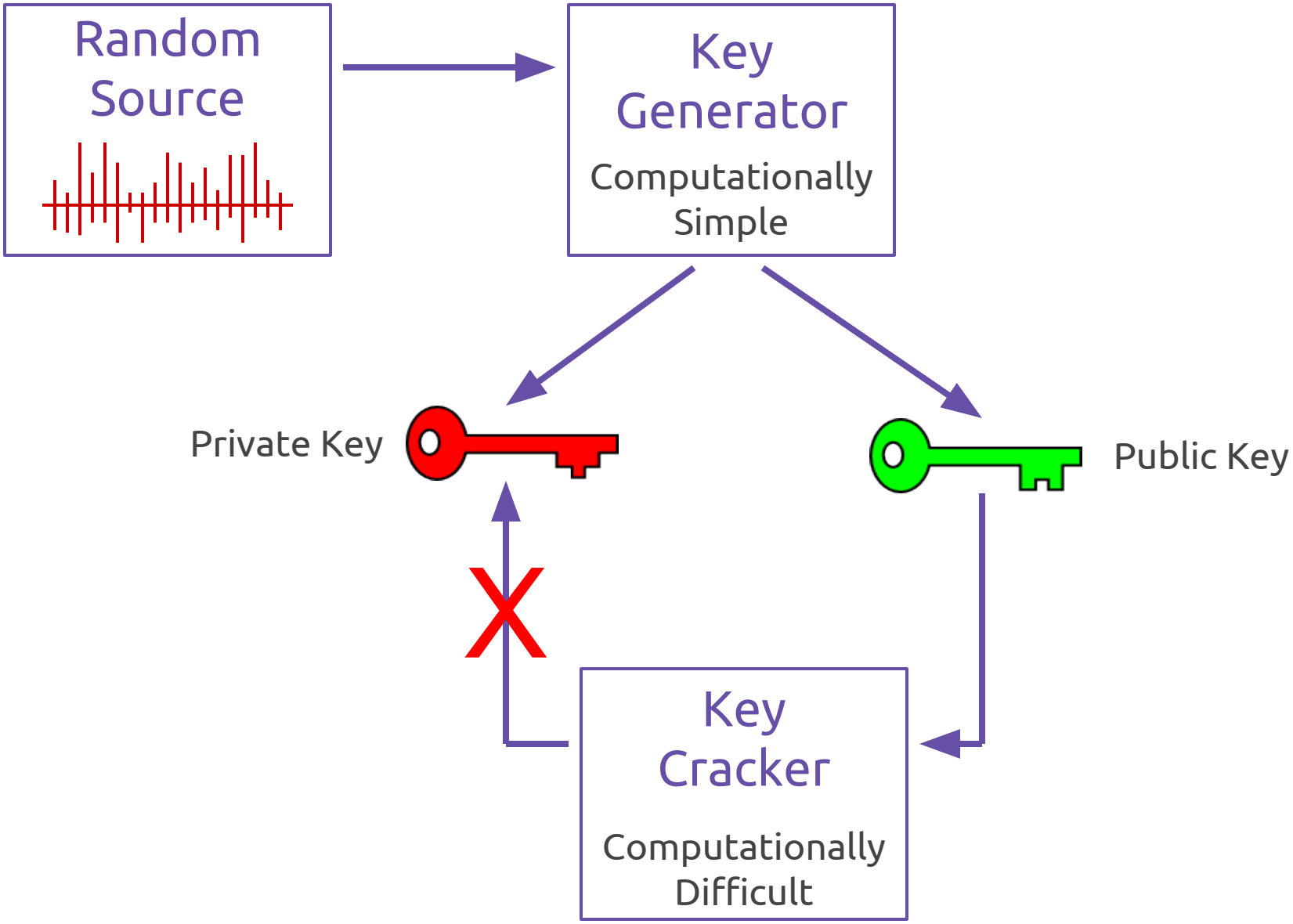
PGP (1991)

Attribute-Based Encryption (2006)

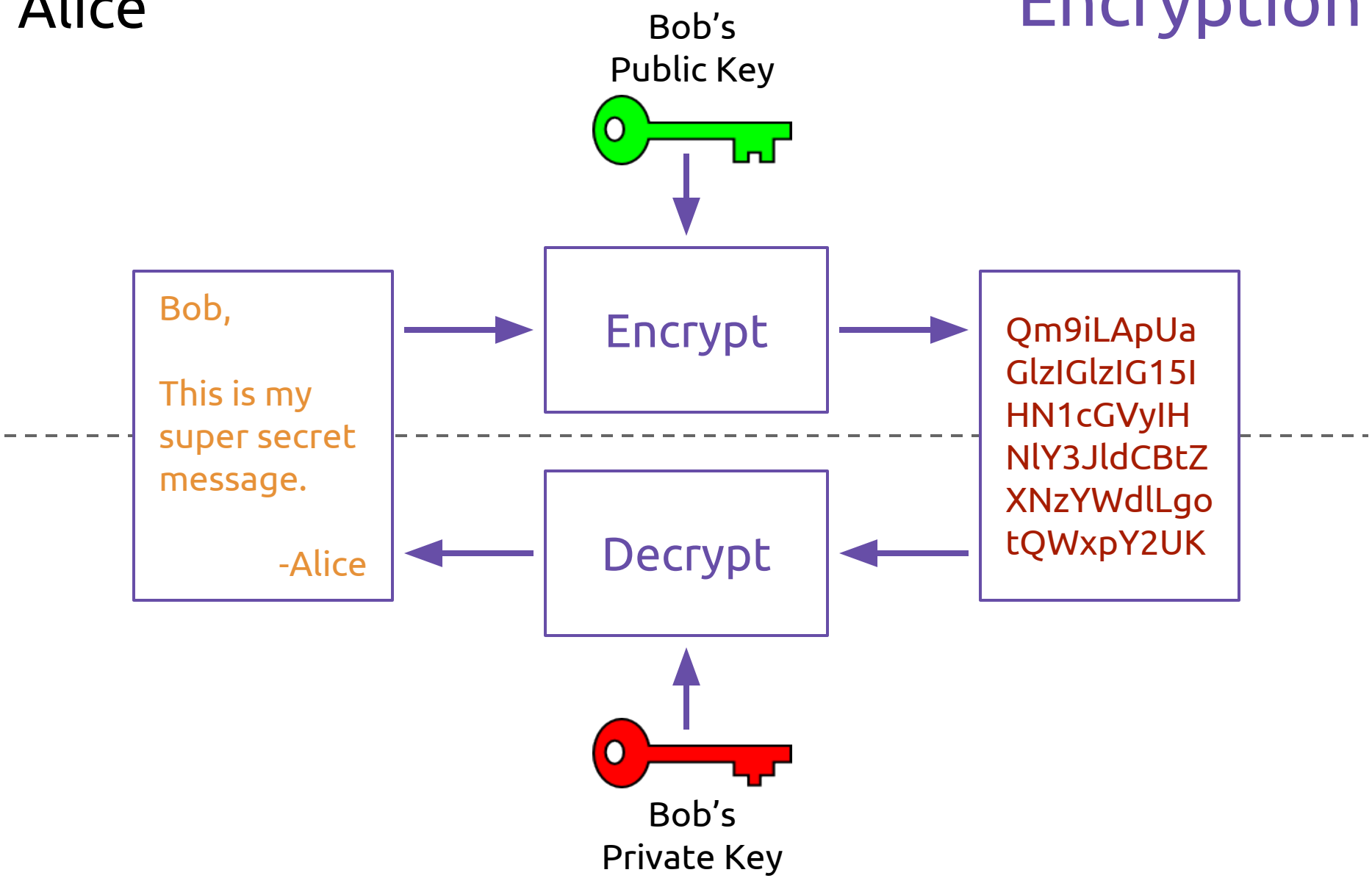
Bitcoin and “Proofs of Work” (2009)

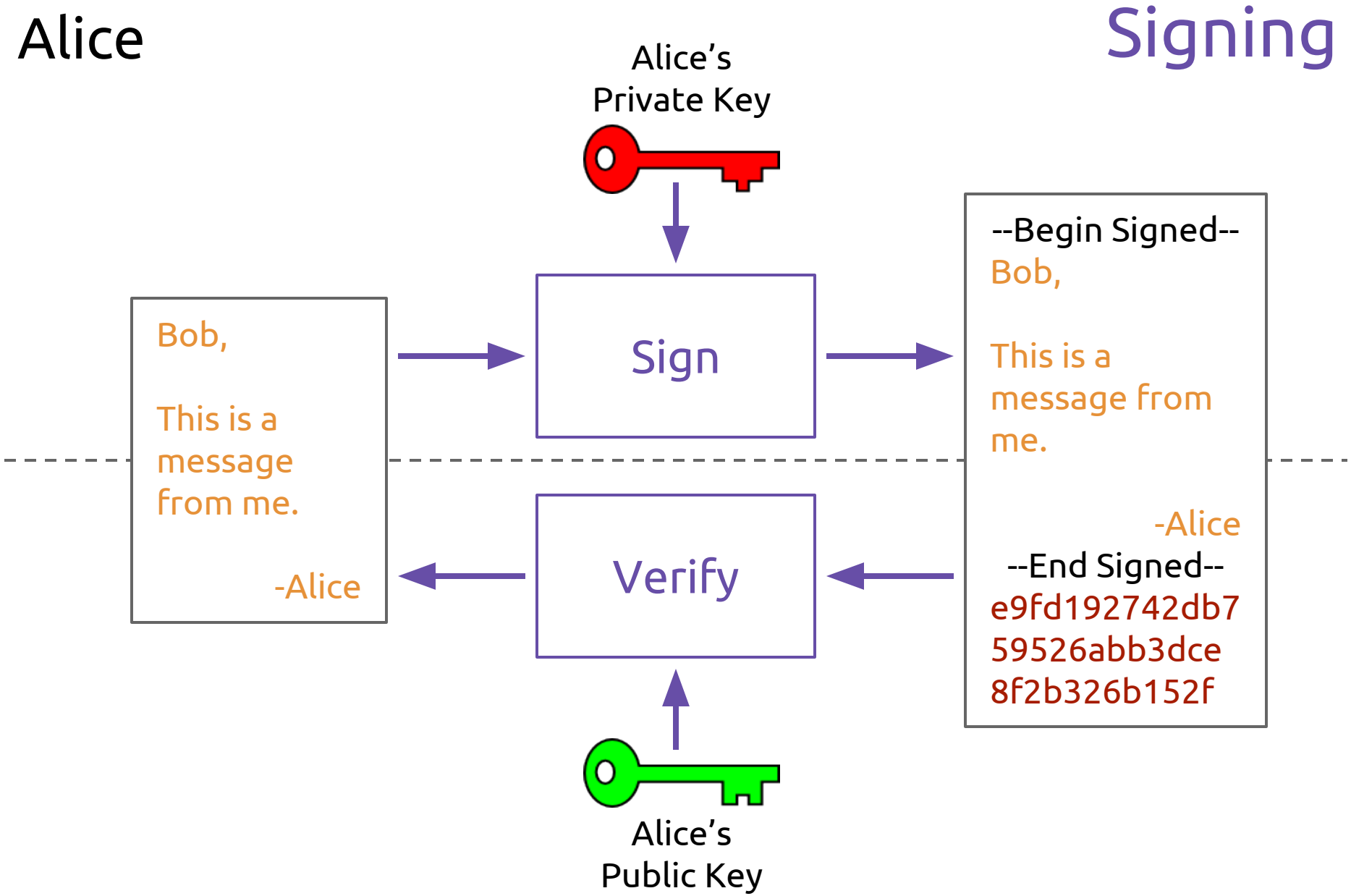

Encrypt
"My Secret"
TXkgU2VjcmV0
Decrypt

Diffie & Hellman.
New Directions in Cryptography.
IEEE Transactions on Information Theory
22, 6. 1976.

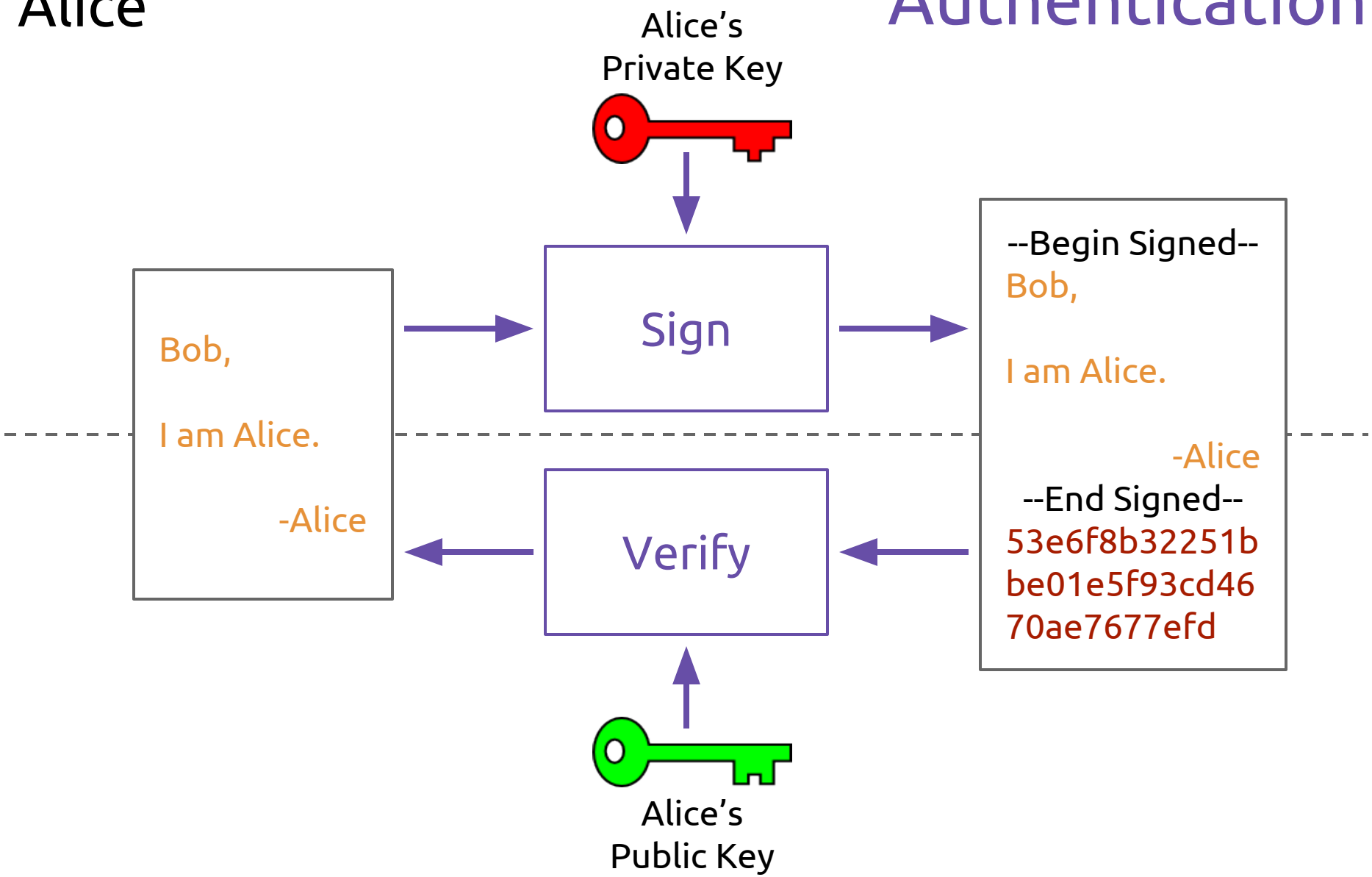

Random Source
Key Generator
Computationally Simple
Private Key
Public Key
Key Cracker
Computationally Difficult

Encryption

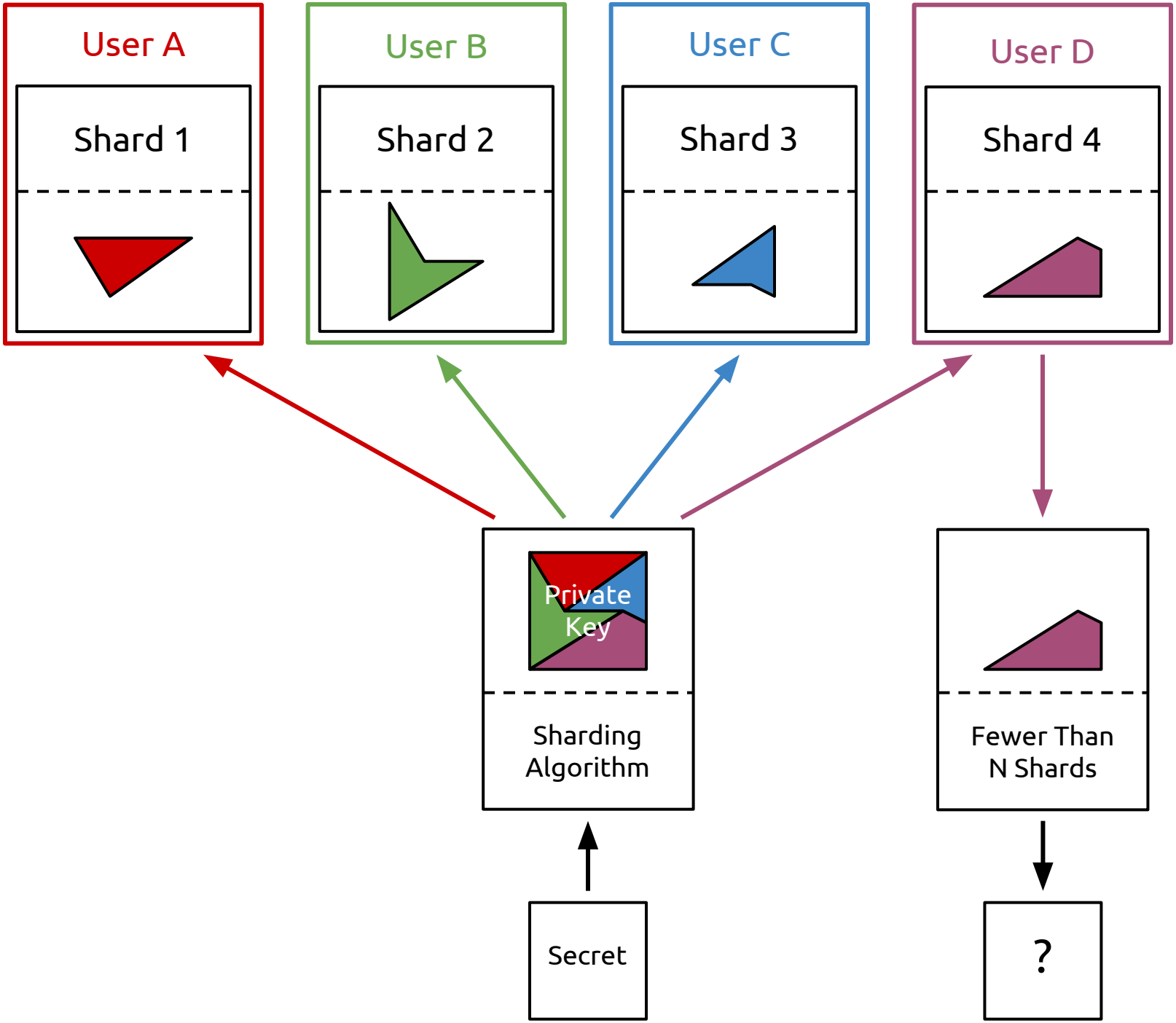

Alice
Bob's
Public Key
Bob,
This is my
super secret
message.
-Alice
Encrypt
Qm9iLApUa
GlzIGlzIG15I
HN1cGVyIH
NlY3JldCBtZ
XNzYWdlLgo
tQWxpY2UK
Decrypt
Bob's
Private Key
Bob

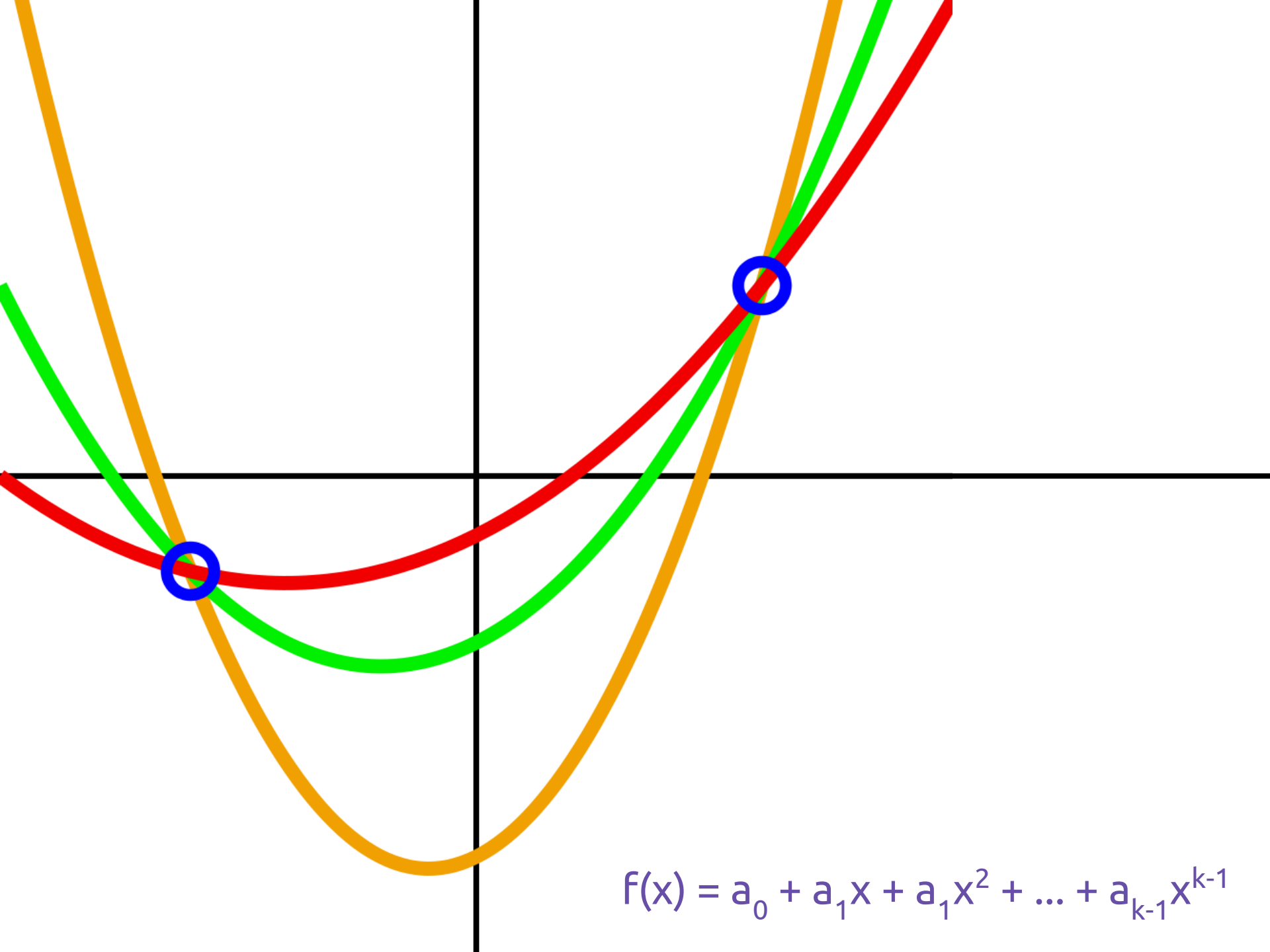

Alice
Signing
Alice's
Private Key
Bob,
This is a
message
from me.
-Alice
Sign
--Begin Signed--
Bob,
This is a
message from
me.
-Alice
--End Signed--
e9fd192742db7
59526abb3dce
8f2b326b152f
Verify
Alice's
Public Key
Bob

Authentication



Shamir, Adi.
How to Share a Secret.
Communications of the ACM
22, 11. 1979.


User A
Shard 1
User B
Shard 2
User C
Shard 3
User D
Shard 4
Private Key
Sharding Algorithm
Fewer Than N Shards
Secret
?


$f(x) = a_0 + a_1x + a_1x^2 + \ldots + a_{k-1}x^{k-1}$

The Future

Quantum Cryptography (?)

Sourcing Randomness/Entropy

Secure Secret/Private Key Storage

Access Control

Time Sharing OSes (1950s to 1960s)

Multics (1969)

Unix + Unix File Permissions (1973)

Linux (1991)

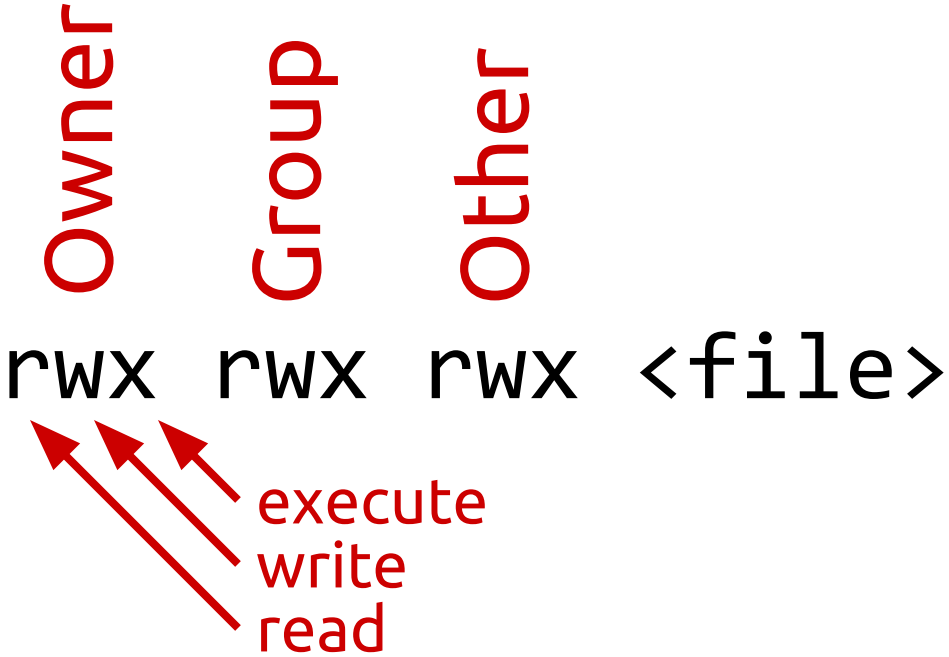
Windows NT + ACLs (1993)

Role-Based Access Control (1996)

Key-Policy Attr-Based Ecypt (2006)

Ciphertext-Policy Attr-Based Ecypt (2007)

Unix Permissions



Windows NT ACLs

```
<file>
|--- read: (User A, User B)
|--- write: (User A, User B)
|--- delete: (User A)
|--- change perms: (User A)
|--- ...
```

Sandhu, et. al.
Role-Based Access Control Models.
IEEE Computer
29,2. 1996.

" We can solve any problem by adding an additional level of indirection... "

" ... except for the problem of too many levels of indirection. "

Users → Permissions

Users →

Users $\rightarrow$ Roles

Users $\rightarrow$ Roles

Roles $\rightarrow$

Users → Roles

Roles → Permissions

```
Roles
|--- Admin: (User A)
|--- Developer: (User A, User B)
|--- ...

<File>
|--- read: (Admin, Developer)
|--- write: (Admin, Developer)
|--- delete: (Admin)
|--- ...
```

$RBAC_0$: Base Model

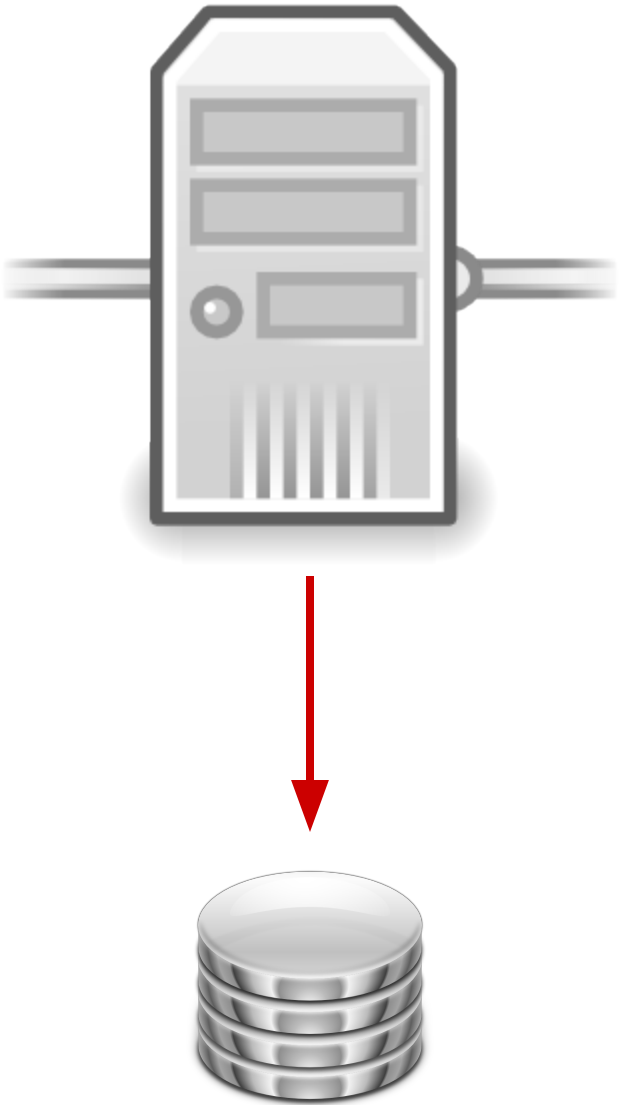
$RBAC_1$: Base Model + Role Hierarchies

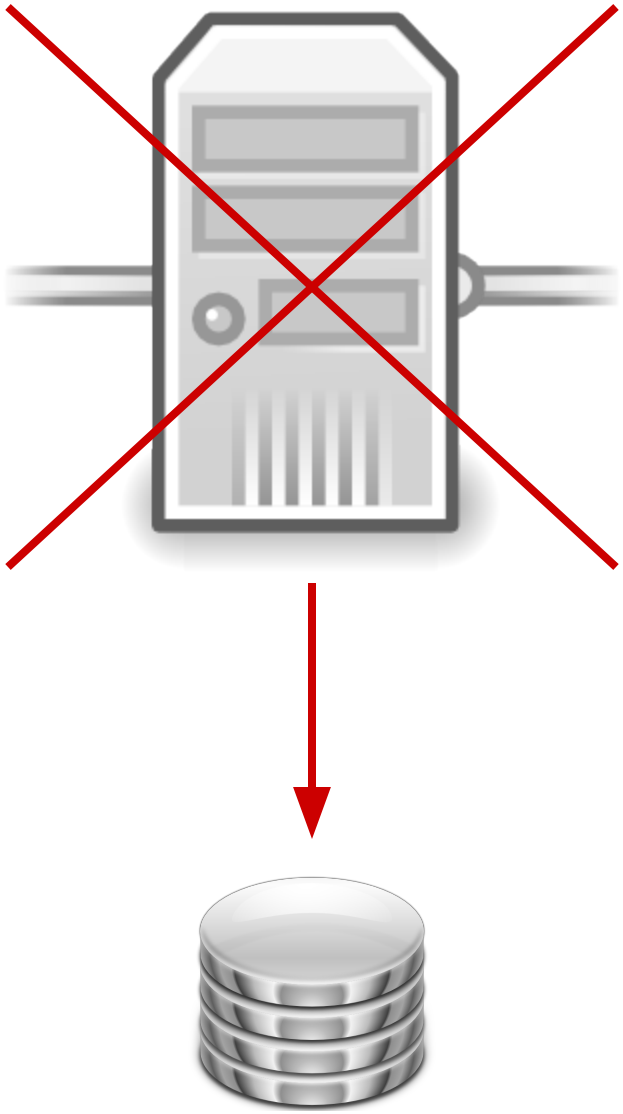
$RBAC_2$: Base Model + Constraints

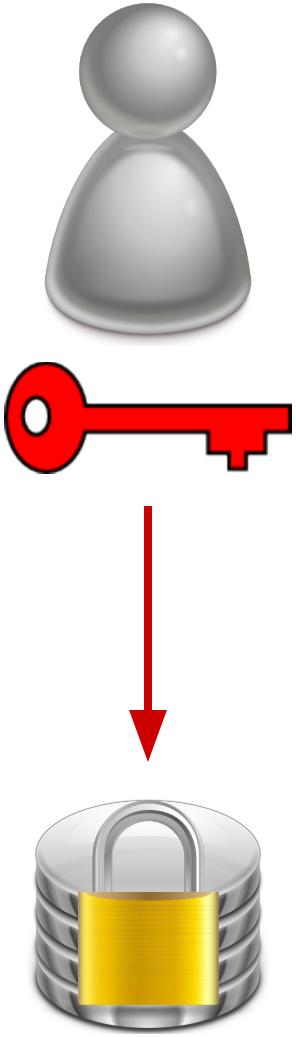
$RBAC_3$: $RBAC_1$ + $RBAC_2$

Bethencourt, et. al.
Ciphertext-Policy Attribute-Based Encryption.
IEEE Symposium on Security and Privacy. 2007.

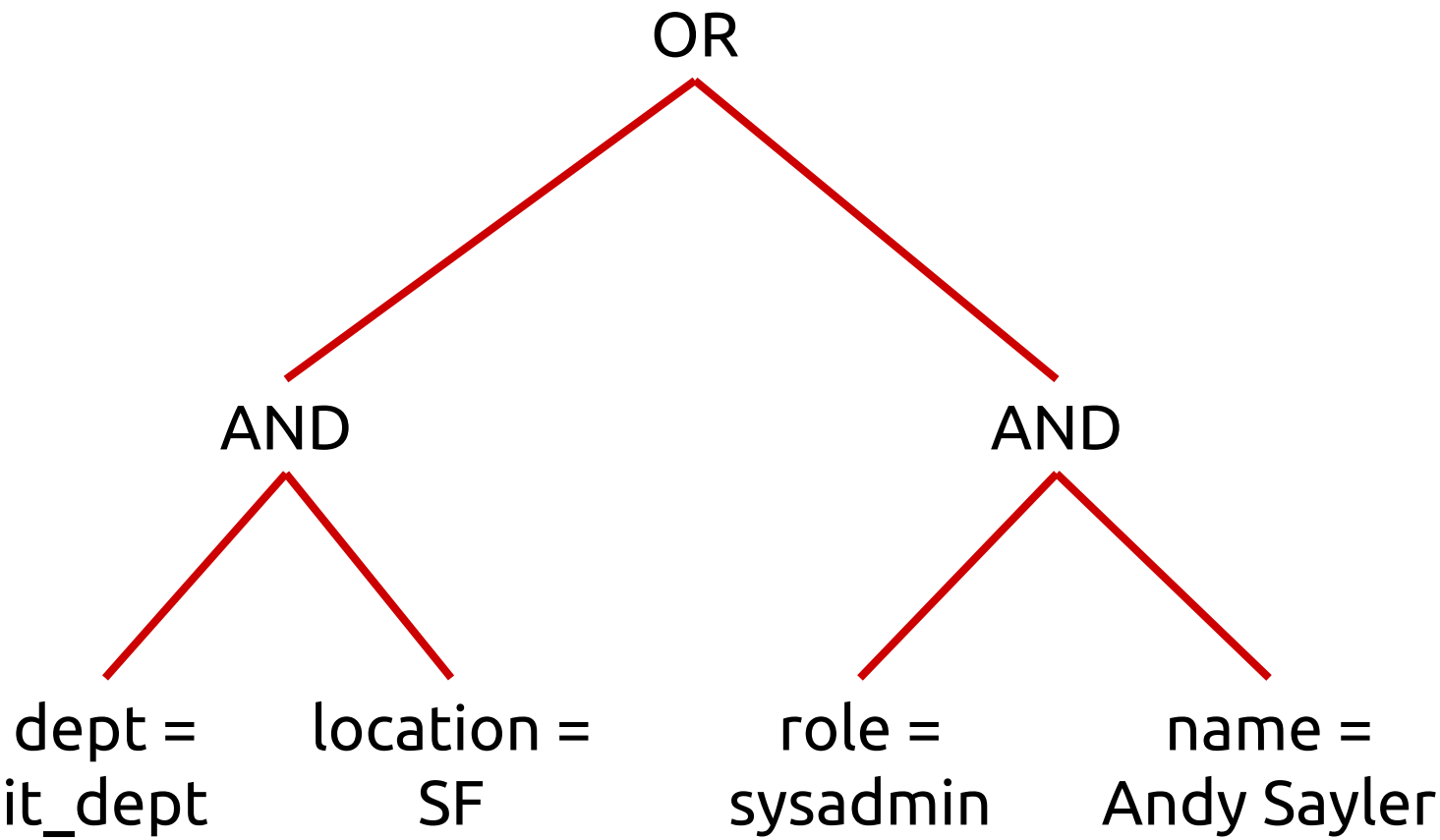
```
(
 (“dept = it_dept”)
 AND
 (“location = “SF”)
)
OR
(
 (“role” = sysadmin)
 AND
 (“name = Andy Sayler”)
)
```







```
|--- “name = Andy Sayler”
|--- “role = sysadmin”
|--- “dept = it_dept”
|--- “location = Boulder”
|--- “hire_date = 09/06/2013”
```


OR
AND
AND
dept =
it_dept
location =
SF
role =
sysadmin
name =
Andy Sayler

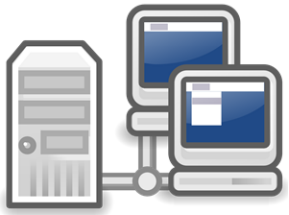
The Future

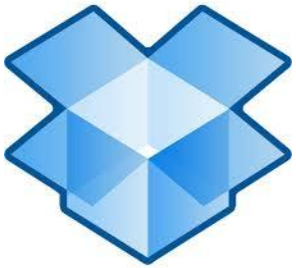
Global Namespaces

Authentication vs Authorization

Manageability and Misconfiguration

Data Storage Security



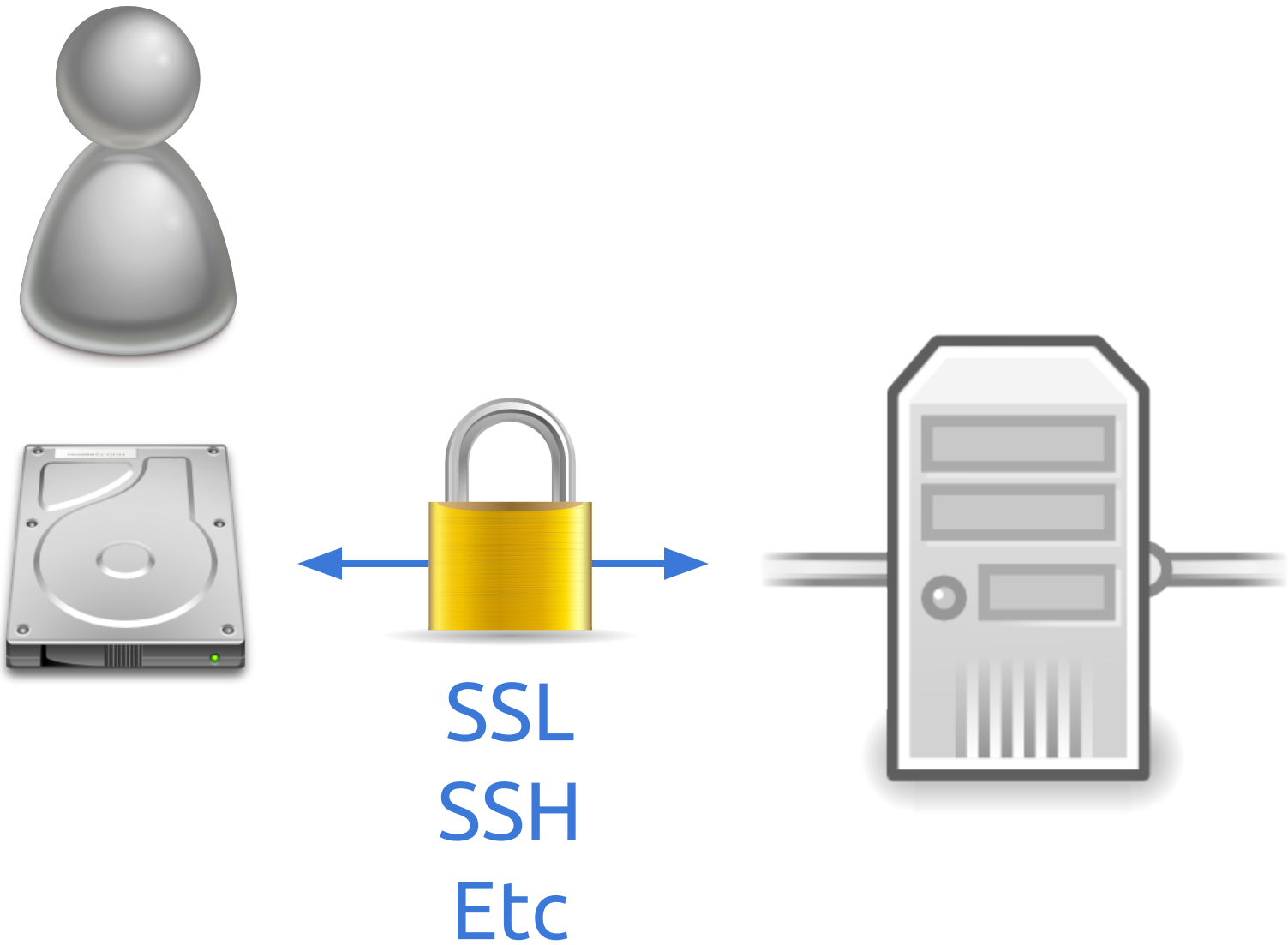


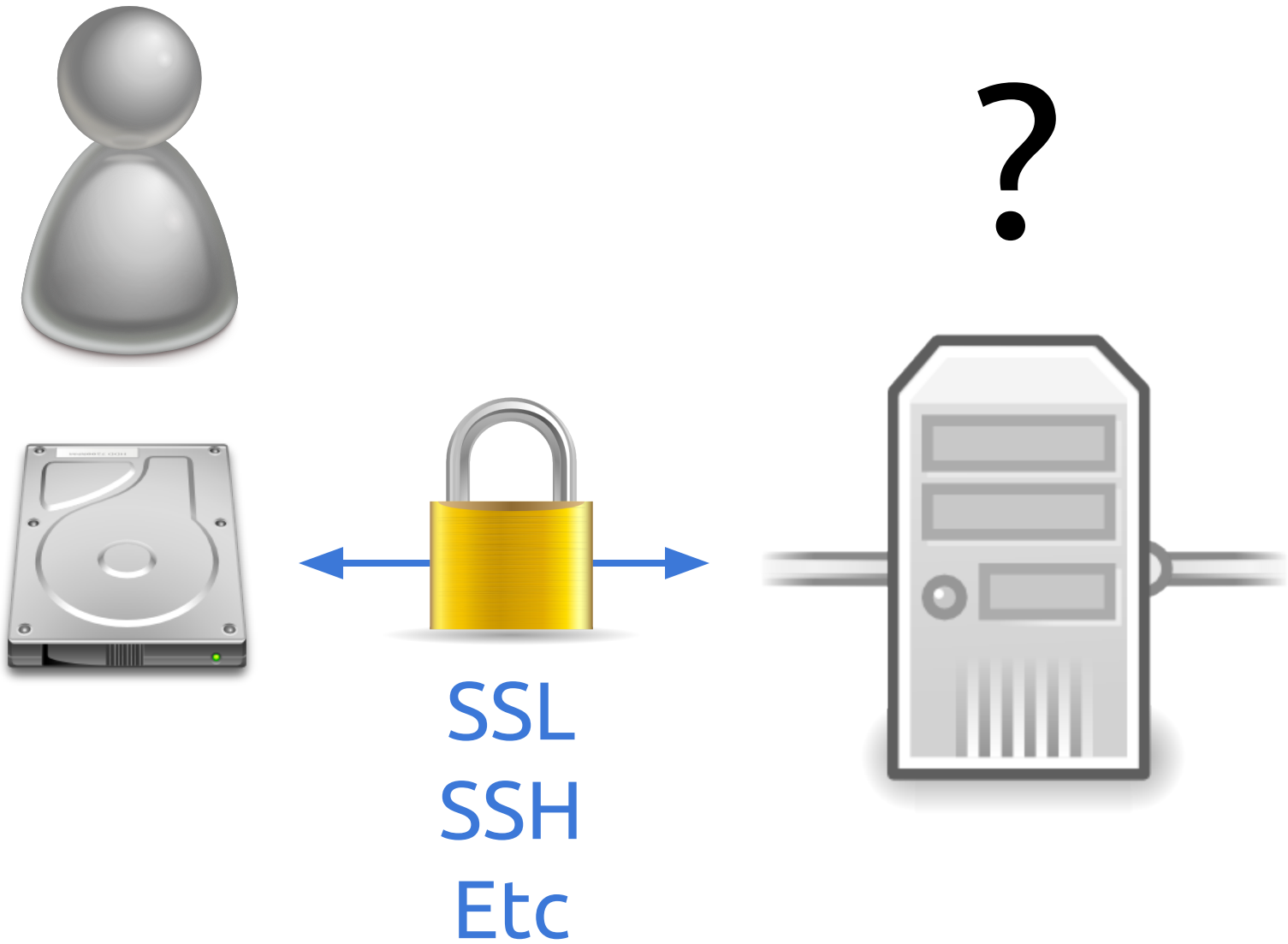
- Unix (1973)
- NFS (1984)
- Andrew File System (1988)
- SMB (1990)
- Linux (1991)
- NTFS (1993)
- Bayou, CFS (1993)
- CIFS (1996)
- SFS, CryptFS (1999)
- OceanStore (2000)
- Plutus (2003)
- eCryptFS (2006)
- BitLocker (2007)
- Dropbox (2008)

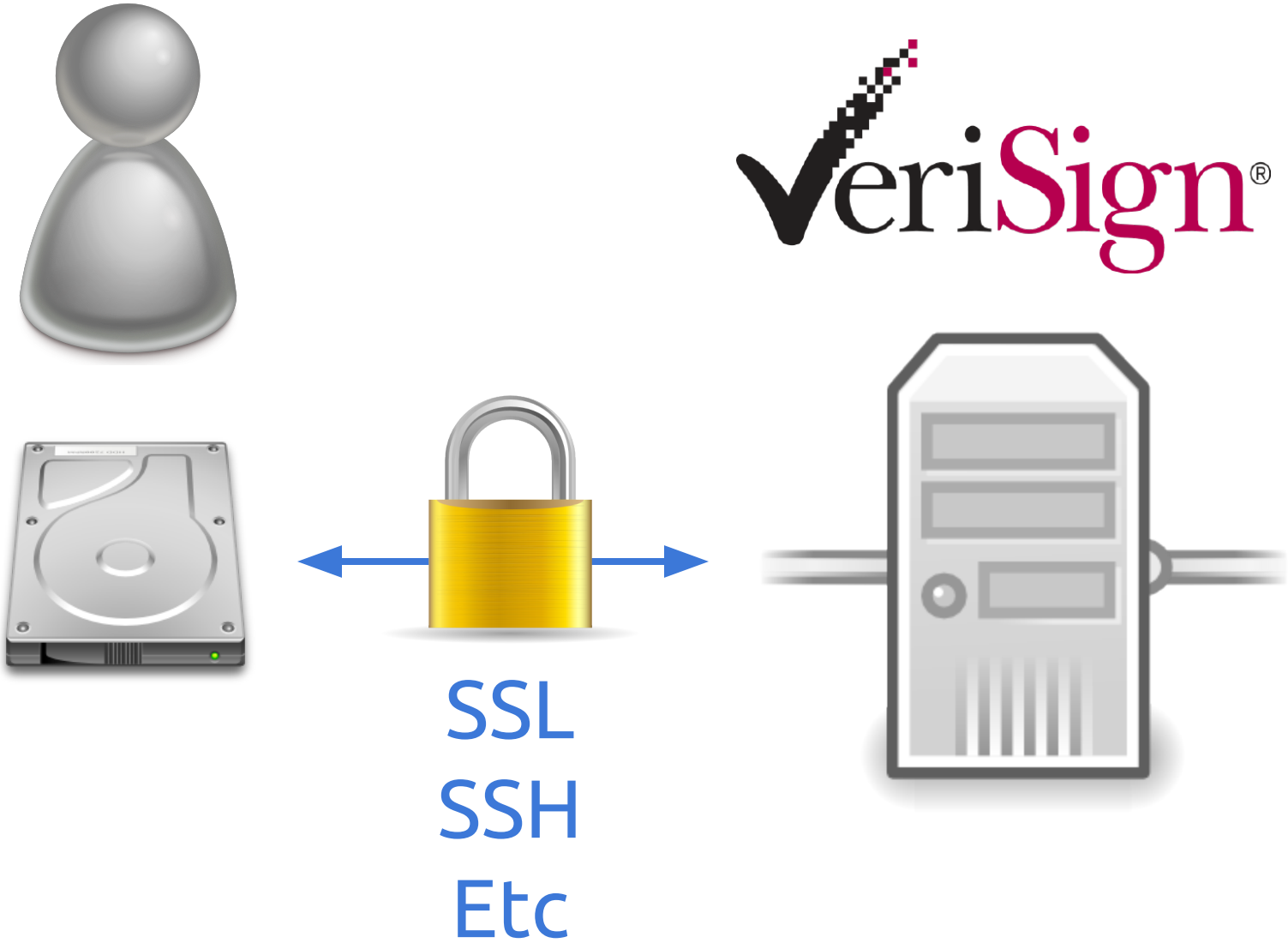
Mazières, et. al.

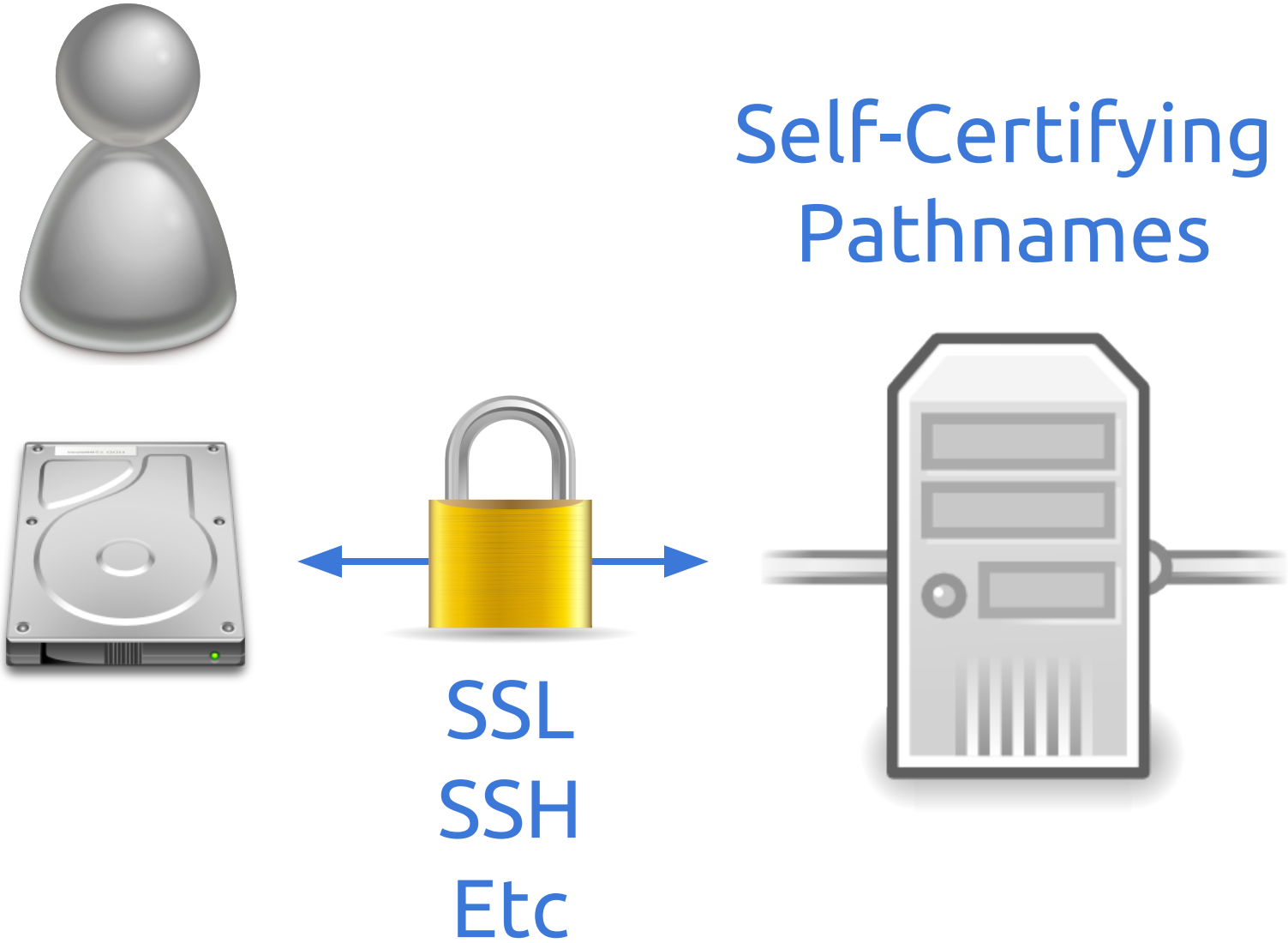
Separating Key Mgmt from FS Security.

ACM SIGOPS Operating Systems Review 33, 5. 1999.


SSL
SSH
Etc


?
SSL
SSH
Etc


VeriSign®
SSL
SSH
Etc


Self-Certifying
Pathnames
SSL
SSH
Etc

Location HostID Remote Path

/sfs/sfs.volaticus.net:vefvsv5wd4hz9isc/pub/docs/prelim.pdf

Location HostID Remote Path

/sfs/sfs.volaticus.net:vefvsv5wd4hz9isc/pub/docs/prelim.pdf

HostID = SHA1(“HostInfo”, *Location*, *PublicKey*)

Kher & Kim.

Securing Distributed Storage:

Challenges, Techniques, and Systems.

Proceedings of the 2005 ACM Workshop on Storage Security and Survivability

2005.

Miltchev, et. al.

Decentralized Access Control in Distributed File Systems.

ACM Computing Surveys

40, 3. 2005.

Distributed File Systems

Single Domain

NFS (v1 to v4)
AFS
CIFS/SMB
Bayou
xFS

Multi Domain

SFS
OceanStore
DisCFS
Truffels
WebFS
CapaFS
Fileteller
TahoeFS
DisCFS

Cryptographic File Systems

Single User

CFS
CryptFS
eCryptFS
TrueCrypt

Multi User

TCFS
NCryptFS
EFS
SFS
GFSF
SiRiUS
Cephus
Plutus
TahoeFS

Secure File System Attributes

User, System, and Message Authentication

Access Control

End-to-End Confidentiality (Data and Metadata)

Key Management

Key Storage

Key Revocation

Non-Repudiation

File System Access Control Attributes

Authentication

Authorization

Granularity

Delegation

Revocation

Accountability

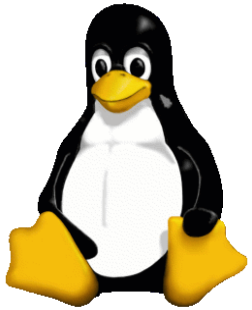
The Future

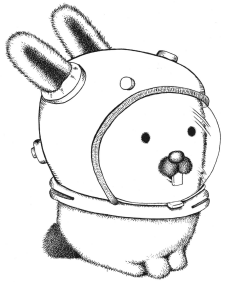
Cloud and Third Party Storage

Multi-Domain, Multi-User, Multi-Device

Usable End-to-End Encryption

Usability and Management





- Kerberos v4 (1988)
- PGP, Linux (1991)
- GSSAPI (1993)
- Kerberos v5 (1994)
- Plan 9 from Bell Labs (1995)
- PAM, RBAC, SSH Agent (1996)
- Why Johnny Can’t Encrypt, GnuPG (1999)
- SAML (2001)
- Security in Plan 9 (2002)
- Shibboleth, OpenID (2003)
- LastPass (2008)

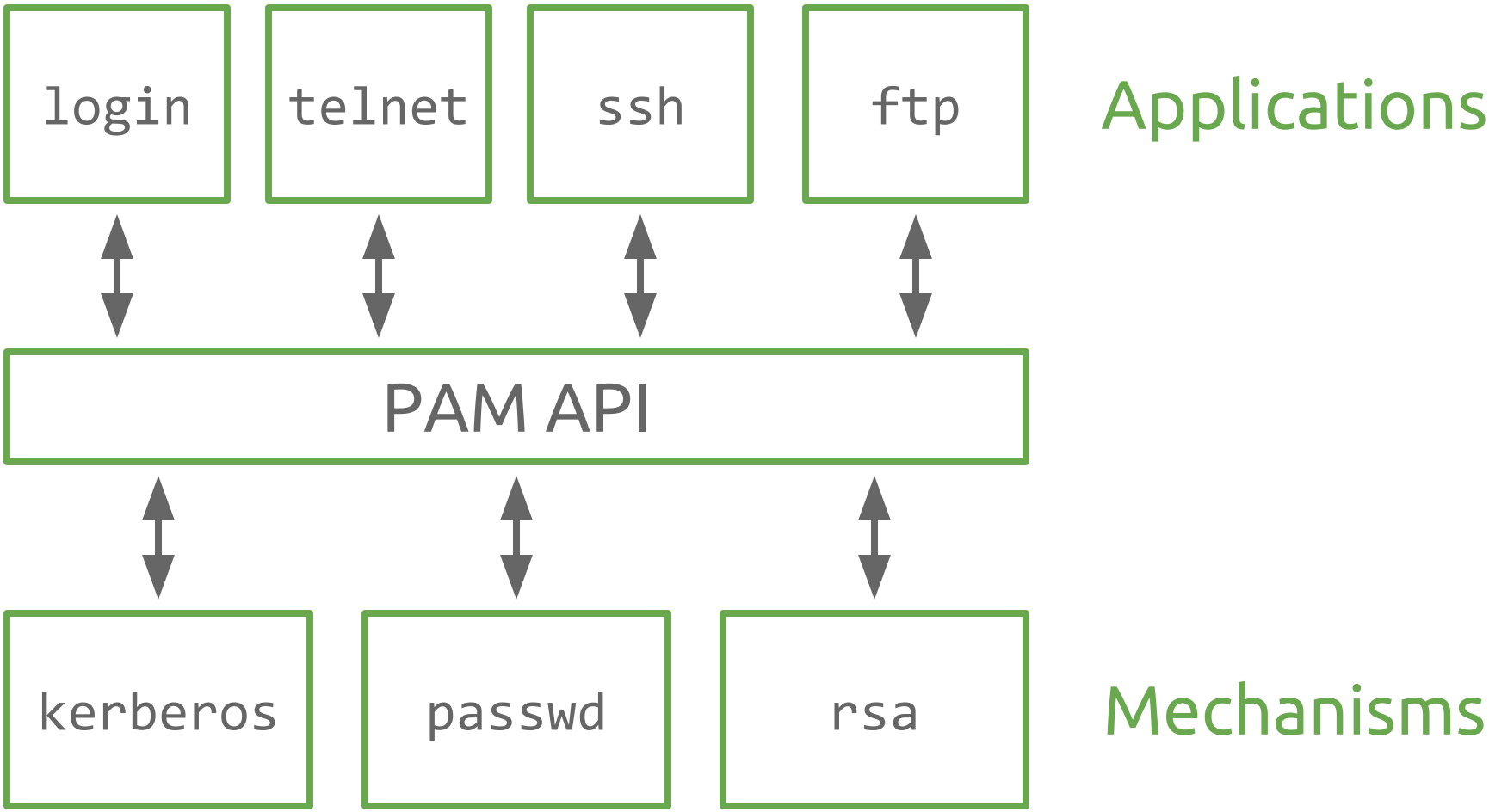
Usability Stakeholders

End Users - How easy is it to use?

Developers - How easy is integration?

Administrators - How easy is management?

Samar, V.
Unified Login with Pluggable Authentication Modules.
Proceedings of the 3rd ACM Conference on Computer and Comm Security.
1996.


login
telnet
ssh
ftp
Applications
PAM API
kerberos
passwd
rsa
Mechanisms

End Users

- Largely transparent
- Provides SSO options

Developers

- Avoids building ad-hoc auth stacks

Administrators

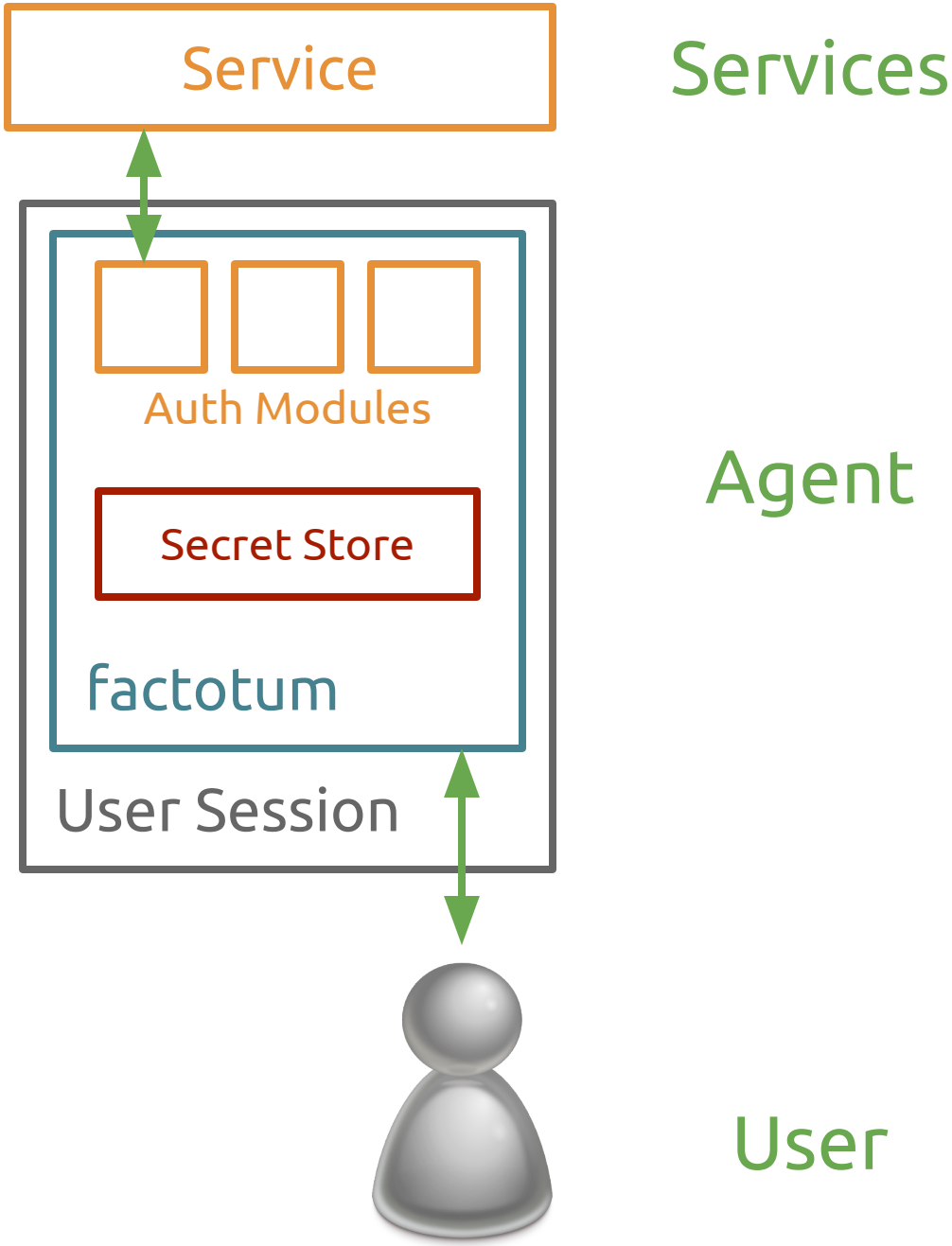
- Select which auth primitives to use
- Provides SSO options

Cox, et. al.

Security in Plan 9.

USENIX Security.

2002.


Service
Services
Auth Modules
Secret Store
factotum
User Session
Agent
User

End Users:

- Avoid need to memorize passwords, etc
- Encourages use of stronger auth techniques

Developers:

- Allows use of stronger auth techniques
- Largely transparent

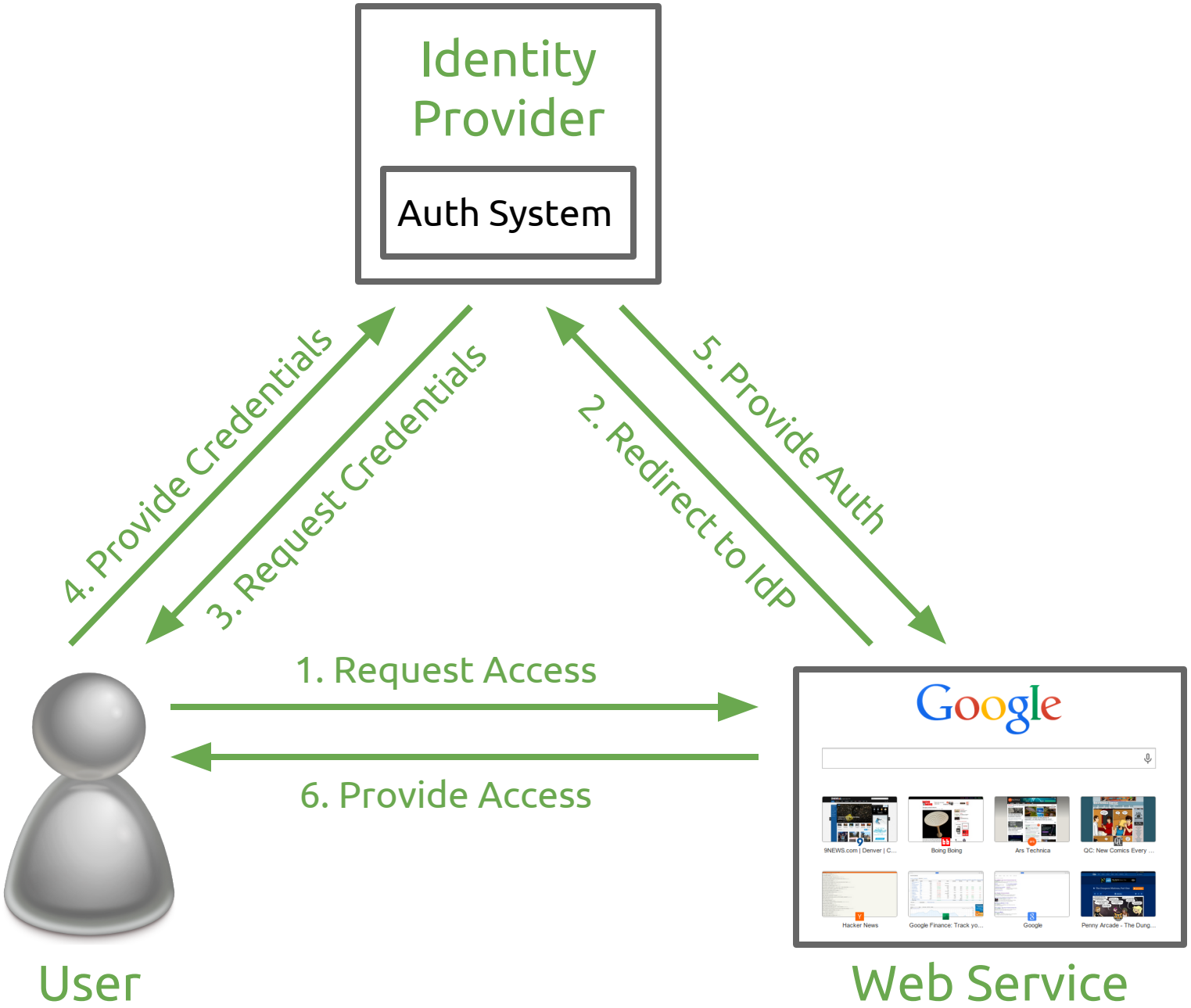
Administrators:

- Largely transparent

Morgan, et. al.

Federated Security: The Shibboleth Approach.

Educause Quarterly. 27, 4. 2004.


Identity Provider
Auth System
4. Provide Credentials
3. Request Credentials
2. Redirect to IdP
5. Provide Auth
1. Request Access
6. Provide Access
Google
User
Web Service

End Users:

Enables SSO to many sites and services

Must only provide credentials to trusted IdP

Developers:

Avoids building ad-hoc auth stacks

Administrators:

Enables SSO for users

Allows centralized control of user attributes

The Future

Security vs Convenience

Multi Domain|User|Device Agents

Third Party Trust and User Control

How can we secure our systems and data in a robust, comprehensive, and easy-to-use manner?

Multi Domain|Device|User Support

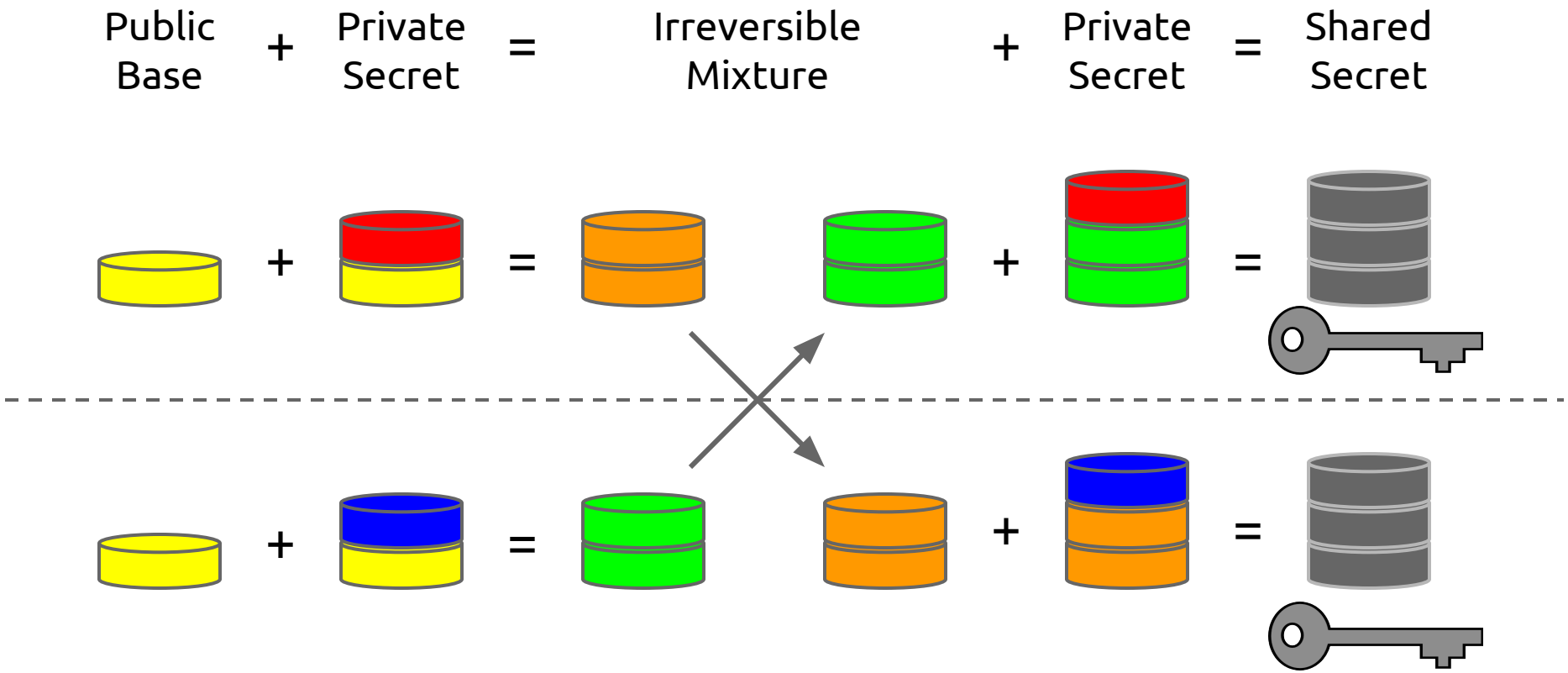
Control over “Who You Trust”

Ease of Use for Users|Devs|Admins

Questions?

Key Exchange

Alice



Bob