
csci54 – discrete math & functional programming
relations, RSA

Relations recap

- ▶ A (binary) relation on a set A is a subset of $A \times A$
- ▶ A relation can be any, or none, of the following:
 - ▶ reflexive
 - ▶ symmetric
 - ▶ transitive
- ▶ A relation that is reflexive, symmetric, and transitive is called an equivalence relation
- ▶ An equivalence relation on a set A partitions A into a set of equivalence classes



Practice questions

- ▶ For each of the following relations, indicate if it is reflexive, symmetric, and/or transitive. If it's all three and therefore an equivalence relation, describe the equivalence classes.
 1. $S =$ all juniors and seniors at Pomona. (x,y) in R_1 iff x and y share a major.
 2. $S = \mathbb{Z}$. (x,y) in R_2 iff $x=y$.
 3. $S = \{1,2,3,4,5\}$. $R_3 = \{\langle 1, 5 \rangle, \langle 2, 2 \rangle, \langle 2, 4 \rangle, \langle 4, 1 \rangle, \langle 4, 2 \rangle\}$.
- ▶ $S =$ all students at Pomona. Define an equivalence relation on S that isn't one of the ones discussed in lecture last time.



Closures

Definition 8.11: Reflexive, symmetric, and transitive closures.

Let $R \subseteq A \times A$ be a relation. Then:

The *reflexive closure* of R is the smallest relation $R' \supseteq R$ such that R' is reflexive.

The *symmetric closure* of R is the smallest relation $R'' \supseteq R$ such that R'' is symmetric.

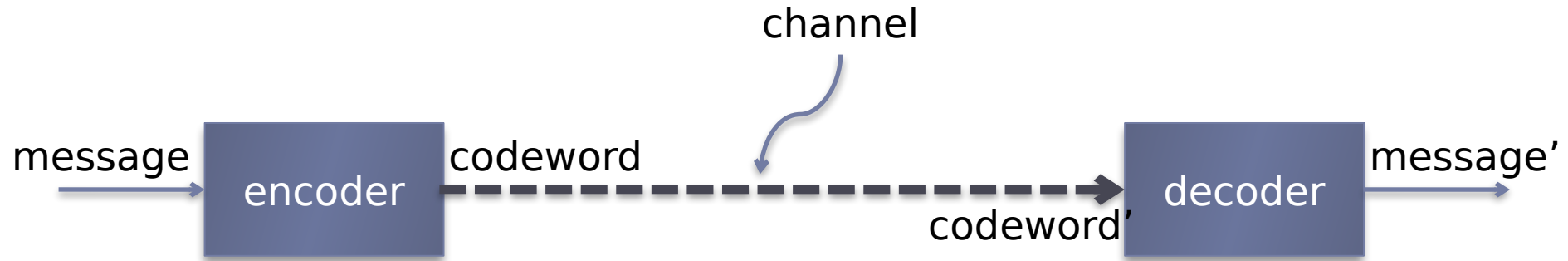
The *transitive closure* of R is the smallest relation $R^+ \supseteq R$ such that R^+ is transitive.

- ▶ Consider the relation $R = \{\langle 1, 5 \rangle, \langle 2, 2 \rangle, \langle 2, 4 \rangle, \langle 4, 1 \rangle, \langle 4, 2 \rangle\}$ on $\{1, 2, 3, 4, 5\}$
 - ▶ What is the reflexive closure?
 - ▶ What is the symmetric closure?
 - ▶ What is the transitive closure?
- ▶ $S =$ all students at Pomona. $(x, y) \in R_1$ if x and y share a major.





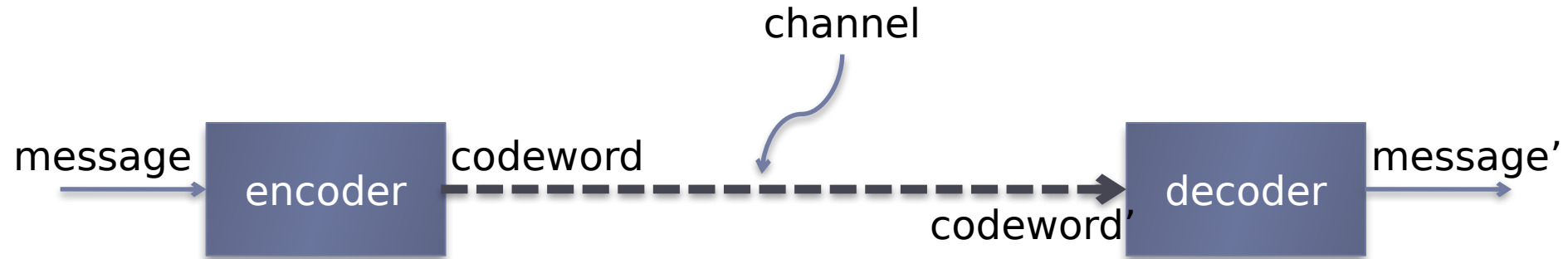
Transmitting information



- ▶ cryptography
- ▶ error correction
- ▶ compression



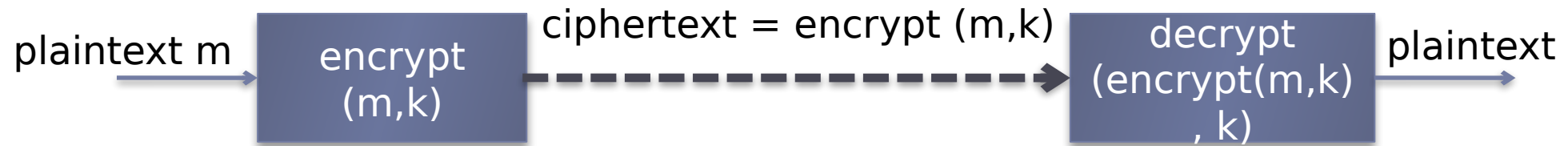
Transmitting information - cryptography



- ▶ goal is to keep someone with access to the channel from finding out information about the message.
- ▶ assumptions (for now)
 - ▶ message = message'
 - ▶ codeword = codeword'
- ▶ why?
- ▶ how?



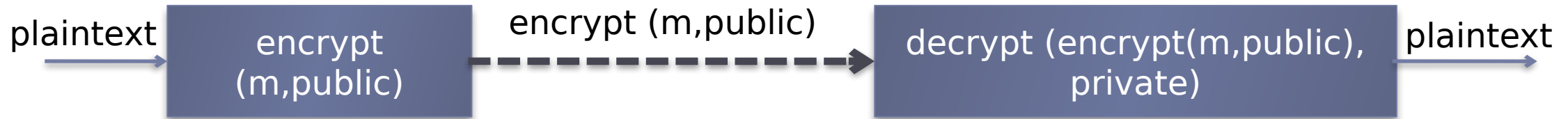
Private key cryptography



- ▶ Symmetric-key algorithms
- ▶ The communicating parties share a piece of secret information (the key k)
- ▶ Examples?
- ▶ Challenges?



Public key cryptography



- ▶ asymmetric-key algorithm
 - ▶ Everyone publishes their public key.
 - ▶ If you want to send a message to someone, you encrypt it with their public key.
 - ▶ When you get a message you can decrypt it with your private key.
-

Public key encryption in practice

A

Richard Adams

Fingerprint: 3DAF 842A DAAF 190D AB13 D701 DCCE B6EA 2697 15E7

Email Address: richard.adams[[@](mailto:richard.adams@theguardian.com)]theguardian.com

[PUBLIC KEY](#)

Esther Addley

Fingerprint: 081E D0F2 4742 3B23 2C53 B0DA FA39 808F D279 4676

Email Address: esther.addley[[@](mailto:esther.addley@theguardian.com)]theguardian.com

[PUBLIC KEY](#)

Jonathan Alden

Fingerprint: 29C6 09D9 5CF7 1EEE 7549 66F6 CD1B 662A 4686 0F81

Email Address: jonathan.alden.freelance[[@](mailto:jonathan.alden.freelance@theguardian.com)]theguardian.com

[PUBLIC KEY](#)

Lorena Allam

Fingerprint: 36D5 D5B6 0ADF FB83 0528 F6AF 5D00 EECE 797E 0CD7

Email Address: Lorena.Allam[[@](mailto:Lorena.Allam@theguardian.com)]theguardian.com

[PUBLIC KEY](#)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.11 (GNU/Linux)

```
mQENBFIfn90BCADxc0hKEUKuzjLajLygK6unrB6mQlFXVcMLO+LE/FIAyJrdTXP2
PqxpDkSsK7H6DcOZaoU03jCxAgmjF9MMMzTFdWYAZHqVLPwJw+ZqgX94pMsRgmTL
SLFAYSiSa/yPukEkmc10CwEKUppJ2s1MvRsmr+t0aqlp0QWllhaCmv0hbEiYsXGc
nbW98hmvQGucXoW+9Y7Xcg6xGvCOGNRduaYcMrjro2io9k5C8Qb2SzoSvWGwKvTd
1wx2lcIqhaA4AlHXWDQJRcrTpVebAYzSnijPbXyZAOKbPkvwApI2pU/6qWAF/3yX
2Ld3MWAOTSIzhgdBDlZsmaSeLNRvt9ATp01ZABEBAAG0LUVzdGhlciBBZGRsZXkg
PGVzdGhlci5hZGRsZXlAdGhlZ3VhcmRpwY4uY29tPokBOAQAIAIqUCUUh833QIb
LwYLCQgHAWIGFQgCCQoLBBYCAwECHgECF4AAcGkQ+jmAj9J5RnbKXWgAgB2sTnnB
n+pUPQmf9tEMA7y7/X5tRdFOPTekmRtczV1qlo+GfATdIQpCVtLm+nKMM6QVka
2nFCs/wzOWAneq+iw9YzFJ10LV0J6f9YJFXldS2EzPv4J44T+7d/y30HW3qdem
v73mXP8YcsCruhK2UEZQn7igL10qgdNfqqpK9h41KvFV3TPWbZ8xTP1hU8qAL
j5AH8OYEdFwN1BMiu7QsKeY5srD3MqvwQ1v3BxbBCN5rx+fbVZ7ie9guCXoMc5mx
qKk+92IzmLE7gDhX0qcvBGsROBFKQlP5RPeIxljuS+GS3JU5QrRtTxhg8Z88jz
IAp2d/tzPBoKUriNBFIfn90BBACp7yZAlMgj+rYvIDK70VJJzbrfxIweBjTUMvVk
16E5Kjr2VoxNMnk5+Ykzi0GSxwP7U2urrtWxe3yJlXCoJp916jvaM92ImlD8FkP4
tmJxuIvmdnHH0+S7eqq286eti18IuHFosFN2tUs9xS8WwYB1aBmbAzujrrkLIvNB
3LzvqWARAQABiQG9BBgBAgAJBQJSHzfdAhsuAKgJEPo5gI/SeUz2nSAEGQCEAAyF
AlIfn90ACgkQt0F2F+VPJGBSmap/d6q4czB+kbaGR15dWHjPO/Si93YzjYAhYhq
w7Bf8Qv2LXiPut1XQRk9EK7P17NnrMxb2oTv7yURIXG+O4qrrvS7lp09yngYULLP
OE2NEcSySfs2ayur1MHdzD+RsyAGLMfPBh4D4w5SSptc5xCzEYie5h8L6APMWGAR
PfcUqe1fwf/ascMLMyHOLeWSq91QaFJN17WiwXBQeXmXFwH2U+R4tjPLWBgceQf
Z8NsTMCQ7t0s0dn5YvblLFhfozQs2u2Q1IS5UQgQwf+XChaw3E9ICdaZRNX9c8f
C17LI3Z7aqbzrDgUU1ox61TO7FZCrSNFSFUpNXhKVXlrTygcdfnbPiqRrsGQR85I
dMvTvFKfQglxQsITF9YkKD8yX3Opy5KR9mL0lg5o1V0z9KEpg2vNpucDc2Nn3DKY
E6oV5JBlQpYh2QGgESY/I/bxz8ZHvoZ7+SH3DZ+ufrXEXzBcAtGHYFhNngikS63EX
z0k5k0ndQnflqoiZ3mncYU8hNntu3SgumSw==
=O+zV
```

-----END PGP PUBLIC KEY BLOCK-----

Encrypted Email

If you use PGP encryption, here is our fingerprint and link to our public key. If you use our public key with a mail encryption plugin, for example Mailvelope or Enigmail, this encrypts the contents of your message but not the subject line or the name of the sender.

Fingerprint:

**EC6C 2905 F0F9 3C03 7394 6CA1 0642
427A 5FF7 80BE**

Email: lockbox@washpost.com

The Post's public key

[Copy](#)

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQGNBGLR6okBDAC7/dy27fxbae1Ss13QI9i93YePYfNjLWJJonVncsmN+ncua
5u8HZJQF09iCytMiZewW6JwCvTFY5TVZcDj/8FTnzpCCFmnczkZP1TVXo5xGL
V7HC3rzpSP8n3vcH0TxcPbBsdzVrzA6QZQDnCiITBYHdfZv7bqT9NGD34mP
b+gmhZbnxZ8YUJ3j7H+Bq3dz2laDl/Hg7+TnfV0GwJuA4uMMPxWtXhZfZv2to
YpuYFg+ptvG0m4FTQEJc88K2xpCl3o0sgg+IhKtpyJ2GF43ee8BBFMcZNSK
xGo7675QYMS8bp9TuBB6GjNeML08EIB50LYfNlAWHx5DBsD5YFGEAnaJnH
3K WrvP5/YvVsa8uYK3gYLU13VW3P8hU7is/h0r0i6prTERuaBkfd5gJlvf
FG+VLB0ZnTnQ4ap7wXV50mje4BACBqWzkyYtuCykdf3J3fYaMyndrnwofIAb
hl q5LcZATSTdApSSAEQEAABQVdQExvY2Iib3ggPgwY2Iib3Ad2FzaHbvc3Qu
Y29tPokB6wQTAQgAPRyHBoXsKQXw+TwDc5RsoQZCQnpf94C+BQJi6+tJAhsDBQ
kD
w7o3BQsJCAcCBhUKCQgLaGQWAgMBAh4A8heAAEJEAZCQnpf94C+FIEE7GwpBf
D5
PANzIGyhBkJCel/3gl5TgQv+P30ainP0IYz2sTLVnInP8d9guhBKvoR1b2k0oA4
IS2g/sONY109CC4SUIUvXqaVLFnDi3x5g/tgW0zV51PKGuKuzimS456Z0ofw
bJuhHc9BypTA7GNqFep7yTL3H1BTeYkWqzTlqAWrvvDzbfjRd4nDgJfHhI
HDEwOun/UFAUK6T855HsZsrhxQxRQ2Gq05plvA9QWmaN7U1et9eZoy2q76bv
6T
Ij2yAse/vN6E4txcPmBF9ZLWHDs+gtpzMWaLqK11tyGwWZjI64ncvS3K70/
NYtnaYjUkIP+fzrIIS8oe8FX3AF0SWYe6hK13GFgceF7AbnIAlyRJSJSvG
yY4yrtUisSP8m5bqJ71Vx1Mw17neEwc5XeZ7ndbVDFD3z0esXG7e/RcGBLz
fuilidJvUwM8718X34ide60w2/6rik41tebQMaCgk4dEduLJIG4rChE2h09uLc
nLxn6PGUqDcaZirBwbn2H5UqGNBGL60kBDACnIsKmY1Hu15IEWUeArFf
4saw/gBYcne2uKQRFfllmq7i6W7I3alEqCaekUZf3sokng5h1PqE7DW+9uz0W9
rpfF2+PakFaTLUcblYdhn/mltXejAdAKVtGJKDE50tV5QpK39dFntm63
t7/G/aFICIAWrrmWzsaKedH+GVXF4NbkH+q6d9hPuxlB9P2wY0e/630JITXq
J
OmugM2BYod9R9kXQY0ZcgTm0XUoHsePhirReWz0tsa16zLiaCgoz5BeqG
w
rBoE9EatesexpAJ7J7Vz0ZjYf4tGXQRkmfKwCwXnTQWAAve1xdwk3YB6cH
Nkn4Waf4TD4Wx+xBadMAOnKv2Vz0BNPmHYsLkN1Lv15FK5nAYN+o26u
OAIFF
o3IMNBwI9QqLTeRhgvwxMeI09UdrV+bxzGIFMDkyrd62b6qW4vTLI6QZT9f9/5
1vNfmTPwIE44IcMhQ64hrDJ7TWstSV+4JDje+EAQEAAyK8owQYAQJhYhBO
XS
KQXw+TwDc5RsoQZCQnpf94C+BQJi6+tJAhsMBQKdW73ACEJEAZCQnpf94C+FIE
E7GwpBfD5PANzIGyhBkJCel/3gl7uXwwAnxcevQFgU7ZmKlZBjCcf4VhITaP
IGMKP1WJ07JpXx9qReYWARkpcWzU16crg8fndAekHgu0tLkRnCJaTnxWUHMqX
+z uOX6I4G5dxlvrk3arqVz48doxNW2ph1u7dV46j3MFTUjJznkI77rUaoCnb20Y
UodR+1LAPLq4U9fdndWd0DwoK6puiALFZHX1PaQDga05RcBPNACPiGhI3Uv
```

<https://www.theguardian.com/pgp>

<https://www.washingtonpost.com/anonymous-news-tips/>

RSA algorithm

- ▶ A very widely used public key encryption algorithm
- ▶ Three algorithmic components
 - ▶ key generation
 - ▶ encryption
 - ▶ decryption
- ▶ Our plan
 - ▶ What is the algorithm?
 - ▶ Why does it work?
 - ▶ How to implement it efficiently?





Modular arithmetic – definitions and properties

$a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

i.e., exists x, y, z in \mathbb{Z} : $a = x * m + z \wedge b = y * m + z$

Some useful facts from Wikipedia:

(if $a_1 \equiv a_2 \pmod{m}$ and $b_1 \equiv b_2 \pmod{m}$):

$a + k \equiv b + k \pmod{m}$ for any integer k (compatibility with translation)

$k a \equiv k b \pmod{m}$ for any integer k (compatibility with scaling)

$k a \equiv k b \pmod{k * m}$ for any integer k

$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$ (compatibility with addition)

$a_1 - a_2 \equiv b_1 - b_2 \pmod{m}$ (compatibility with subtraction)

$a_1 * a_2 \equiv b_1 * b_2 \pmod{m}$ (compatibility with multiplication)

$a^k \equiv b^k \pmod{m}$ for any non-negative integer k (compatibility with exponentiation)

