Introduction to Modern Cryptography

10th lecture:

RSA encryption

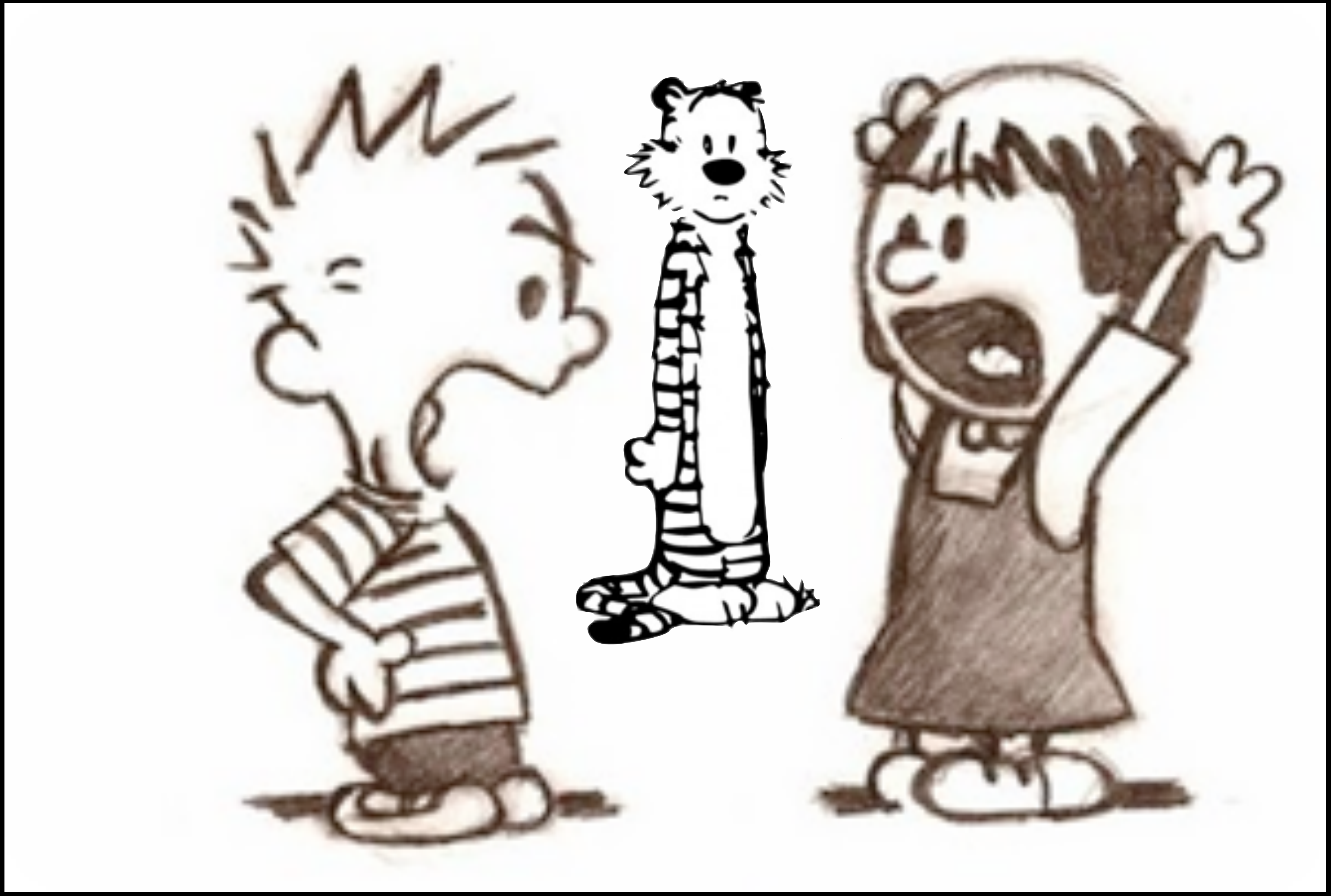
CCA security

last time:

- Definition PubK
- eav => CPA
- multi-message security
- hybrid encryption
- El Gamal

10th lecture (today):

- RSA Encryption
- CCA security



Taher Elgamal

*1955

- 1977: BSc from Cairo university
- 1984: PhD from Stanford
- 1996: "Father of SSL" as Chief Scientist of Netscape
- CTO of various companies

- fun fact: "I read number theory books for fun!"

Ron Rivest

*1947

🇺🇸

Adi Shamir

*1952

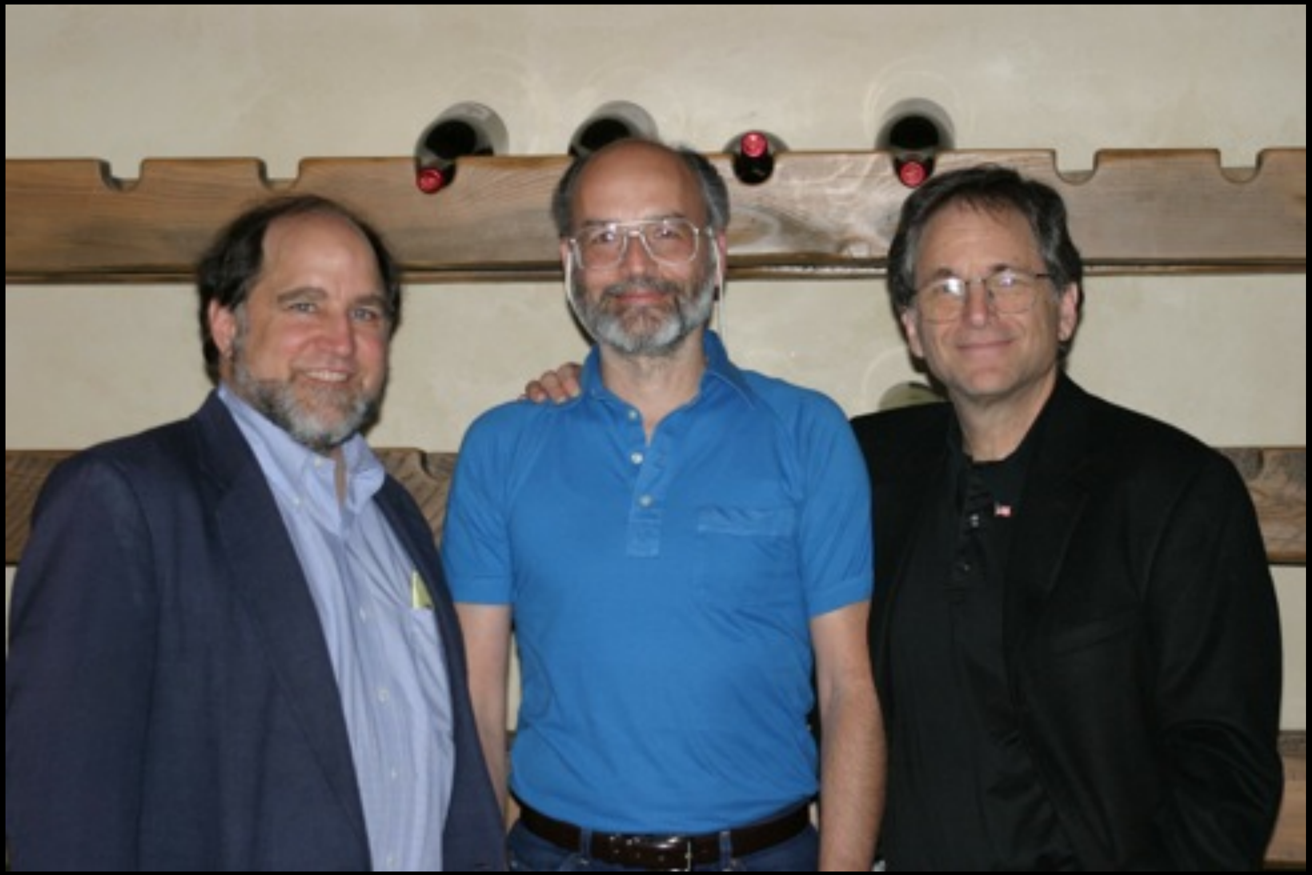
🇮🇱

Leonard Adleman

*1945

🇺🇸

- as MIT students



- in 2003

Insecurity of Textbook RSA

- Textbook RSA is deterministic, thus not even eavesdropper secure!

- weak guarantee under RSA assumption: no PPT adv can recover from the ciphertext the entire message m if chosen at random

- If N can be factored ⇒ RSA problem is easy
- but we do not know if RSA problem is as hard as factoring

Padded RSA

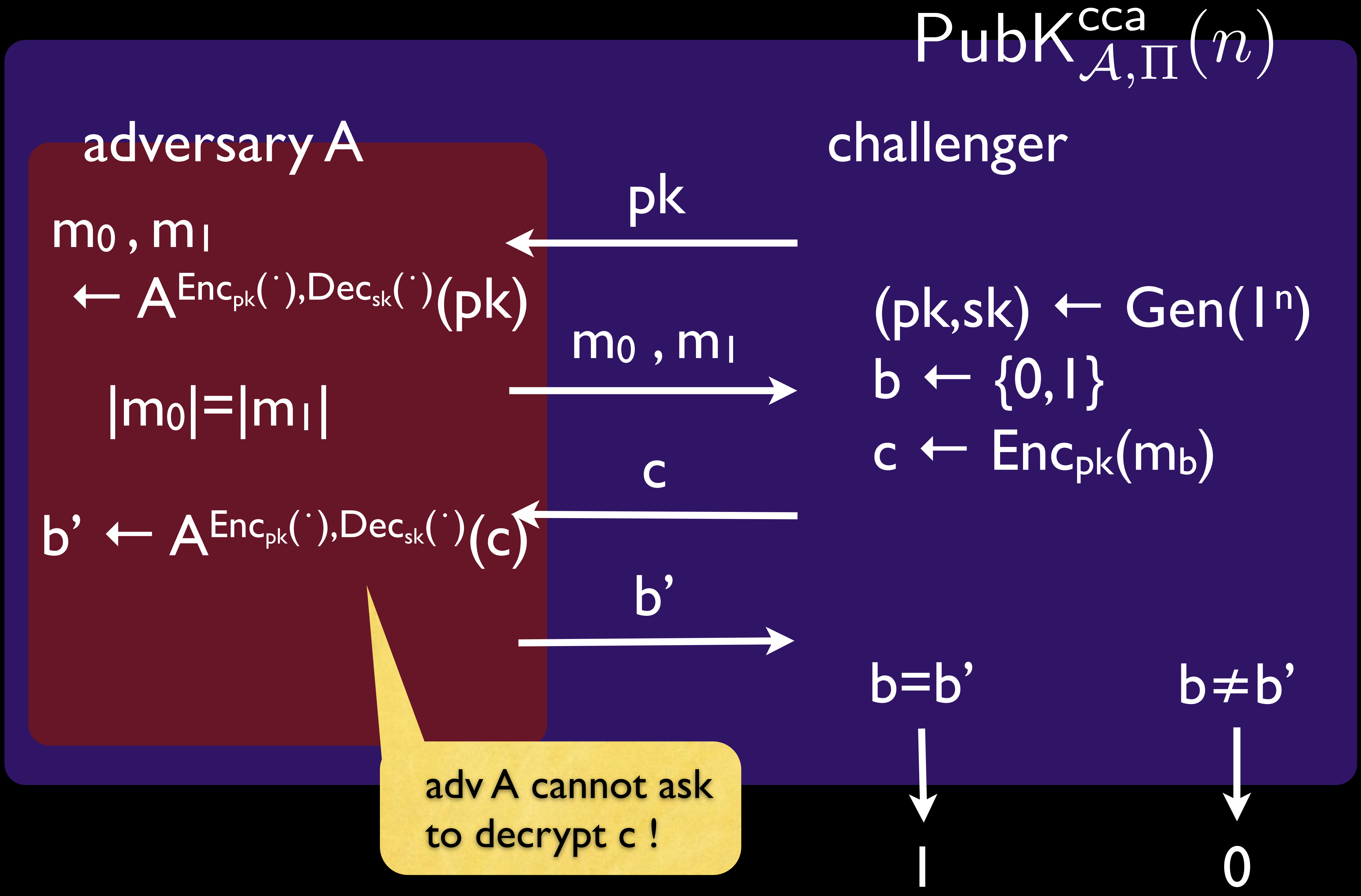
- For $\ell(n) = 2n - O(\log n)$, r can be guessed in polynomial time, not CPA secure
- For $\ell(n) = c \cdot n, c < 2$, padded RSA is conjectured secure, but no proof known
- For $\ell(n) = O(\log n)$, CPA security can be proven

- RSA Labs, Public-Key Crypto Standard PKCS #1, v1.5:

  c := [$(0^8 \,||\, 0^6 10 \,||\, r \,||\, 0^8 \,||\, m)^e$ mod N]

believed to be CPA secure, but CCA-attack is known

CCA security



$\mathrm{PubK}^{\mathrm{cca}}_{\mathcal{A},\Pi}(n)$

adversary A

challenger

pk

m_0 , m_1

$\leftarrow A^{\mathrm{Enc}_{pk}(\cdot),\mathrm{Dec}_{sk}(\cdot)}(pk)$

$(pk,sk) \leftarrow \mathrm{Gen}(1^n)$

m_0 , m_1

$|m_0|=|m_1|$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathrm{Enc}_{pk}(m_b)$

c

$b' \leftarrow A^{\mathrm{Enc}_{pk}(\cdot),\mathrm{Dec}_{sk}(\cdot)}(c)$

b'

$b=b'$

$b\neq b'$

adv A cannot ask
to decrypt c !

1

0

CCA Security Examples

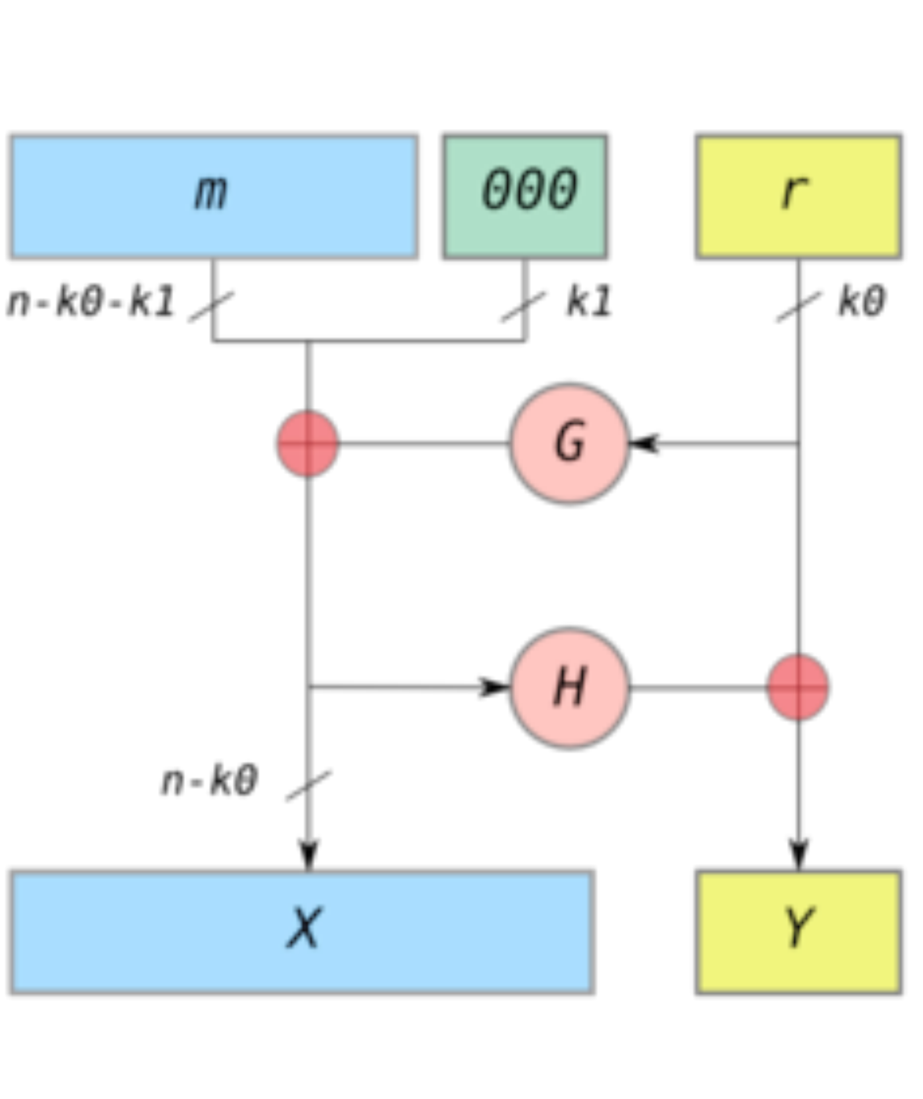
1. Eve intercepts encrypted email to Bob, sends it to Bob herself. Bob answers to Eve and includes the decrypted email (i.e. acts as decryption oracle)

2. Alice & Eve participate in Bob's auction. Alice bids c=Enc(m). Due to CPA security, Eve does not learn m. However, Eve can bid c'=Enc(2m) if Enc is malleable

- CCA-security ⇒ Non-malleability

Optimal Asymmetric Encryption Padding

- Instead of PKCS #1 v1.5 padding, people use RSA-OAEP (Construction 13.9 in [KL])



= $\underline{m}$

Gen: $(N,e,d) \leftarrow \text{GenRSA}(1^{n+1})$

$\|N\| > 2n$

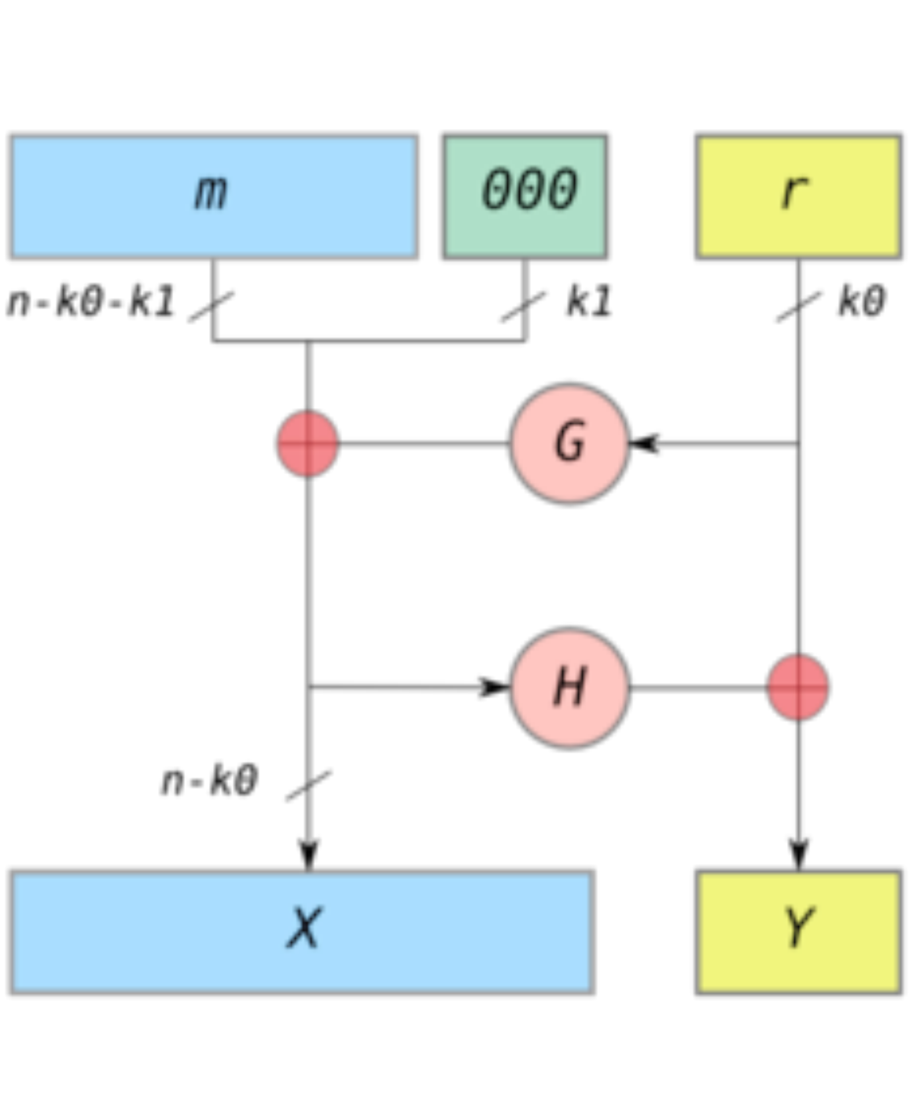
$\text{Enc}_{pk}(m)$: $[\ \underline{m}^e \bmod N\ ]$

$\text{Dec}_{sk}(c)$: $[\ c^d \bmod N\ ] = \underline{m} = X\|Y$

check if final msg is of appropriate form

Optimal Asymmetric Encryption Padding

Thm: If RSA-problem is hard wrt to GenRSA and G,H are independent random oracles. Then, RSA-OAEP is CCA-secure for e=3 (and other exponents)



= $\underline{m}$

Gen: $(N,e,d) \leftarrow \mathrm{GenRSA}(1^{n+1})$

$\|N\| > 2n$

$\mathrm{Enc}_{pk}(m)$: $[\ \underline{m}^e \bmod N\ ]$

$\mathrm{Dec}_{sk}(c)$: $[\ c^d \bmod N\ ] = \underline{m} = X\|Y$

check if final msg is of appropriate form

Recent Software Bugs

- Feb 2014: #gotofail in Apple software
- April 2014: Heartbleed in OpenSSL library, see XKCD
- 24 Sep 2014: Shellshock in Unix Bash shell

Bottom line: implementing security-related software is difficult