

MATH/CMSC 456 :: UPDATED COURSE INFO

Instructor: Gorjan Alagic (galagic@umd.edu)

Guest instructor: Carl Miller (camiller@umd.edu), ATL 3100K

Textbook: *Introduction to Modern Cryptography*, Katz and Lindell;

Webpage: alagic.org/cmsc-456-cryptography-spring-2020/

Piazza: piazza.com/umd/spring2020/cmsc456

ELMS: active, slides and reading posted there.

Gradescope: active, access through ELMS.

TAs (Our spot: shared open area across from **AVW 4166**)

- Elijah Grubb (egrubb@cs.umd.edu) 11am-12pm TuTh (AVW);
- Justin Hontz (jhontz@terpmail.umd.edu) 1pm-2pm MW (AVW);

Additional help:

- Chen Bai (cbai1@terpmail.umd.edu) 3:30-5:30pm Tu (**2115 ATL - inside JOI**)
- Bibhusa Rawal (bibhusa@terpmail.umd.edu) 3:30-5:30pm Th (**2115 ATL - inside JOI**)

Homework 4 was posted today, and is due March 12.

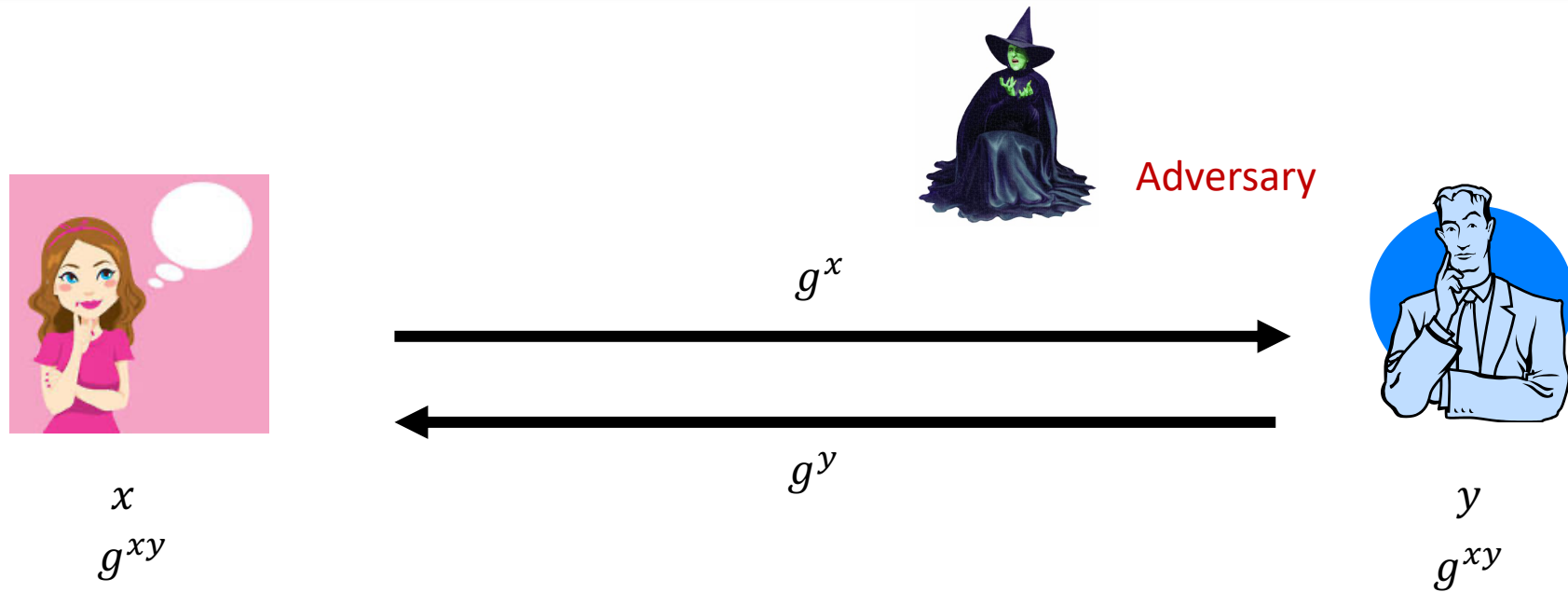
READING FOR TODAY

We were skipping two subsections. I decided to drop **subsection 11.5.4** also. (You won't be responsible for the material there.)

11.4	CDH/DDH-Based Encryption	399
11.4.1	El Gamal Encryption	400
11.4.2	DDH-Based Key Encapsulation	404
11.4.3	*A CDH-Based KEM in the Random Oracle Model	406
11.4.4	Chosen-Ciphertext Security and DHIES/ECIES	408
11.5	RSA Encryption	410
11.5.1	Plain RSA	410
11.5.2	Padded RSA and PKCS #1 v1.5	415
11.5.3	*CPA-Secure Encryption without Random Oracles	417
11.5.4	OAEP and RSA PKCS #1 v2.0	421
11.5.5	*A CCA-Secure KEM in the Random Oracle Model	425
11.5.6	RSA Implementation Issues and Pitfalls	429



RECAP: DIFFIE-HELLMAN KEY EXCHANGE



G = cyclic group with generator g .

Alice chooses random x and sends g^x to Bob.

Bob chooses random y and sends g^y to Alice.

Alice computes $(g^y)^x = g^{xy}$. Bob computes $(g^x)^y = g^{xy}$.

They then have a shared secret.

RECAP: FORMAL MODELS OF PUBLIC-KEY CRYPTO

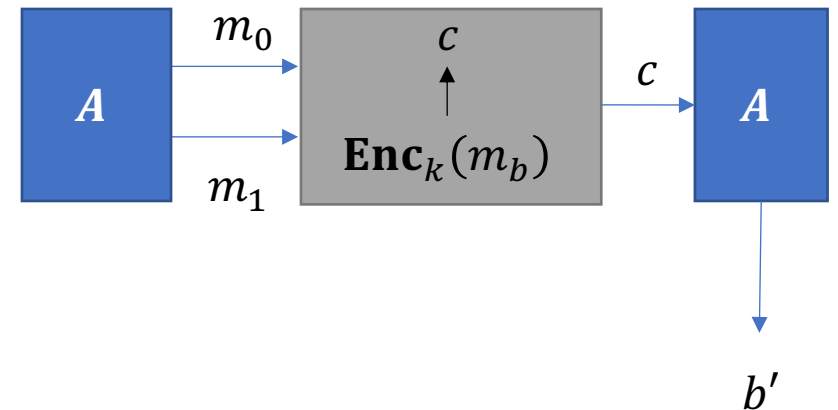
We went through various definitions of security for public-key crypto.

All of them were based on **indistinguishability experiments**.

- **IND-CPA** for public-key encryption
- **IND-CCA** for public-key encryption
- **CPA** for key encapsulation

CPA = "chosen plaintext attack"

CCA = "chosen ciphertext attack"



PLAN FOR TODAY

1. El Gamal encryption

2. RSA encryption revisited.

3. The impact of Shor's algorithm on cryptography.



We are going to overview
some security proofs from the
textbook.

EL GAMAL ENCRYPTION

EL GAMAL (PUBLIC-KEY ENCRYPTION)



x



g^x



Adversary



Let \mathcal{G} be a PPT algorithm that, on input 1^n , generates (G, q, g) .

Size of G

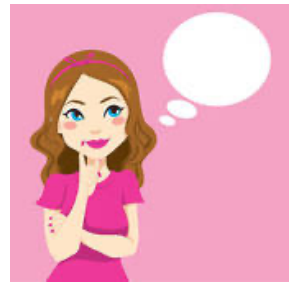
Cyclic group

Generator

Gen: Alice runs \mathcal{G} , broadcasts result.

She chooses random $x \in \{1, 2, \dots, q\}$ and sends g^x .

EL GAMAL (PUBLIC-KEY ENCRYPTION)



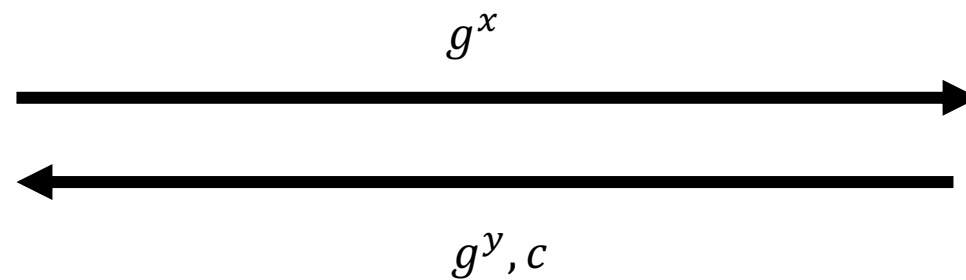
x



Adversary



m



Enc: Bob computes his message $m \in G$.

He chooses random $y \in \{1, 2, \dots, q\}$ and sends g^y **and** $c := (g^x)^y \cdot m$.

Dec: Alice computes:

$$c \cdot [(g^y)^{-1}]^x = g^{xy} m \cdot g^{-xy} = m.$$

Correct decryption is guaranteed by the defining properties of a cyclic group (last lecture).

SECURITY PROOFS

Our security proofs should have:

- Clearly identified algorithms.

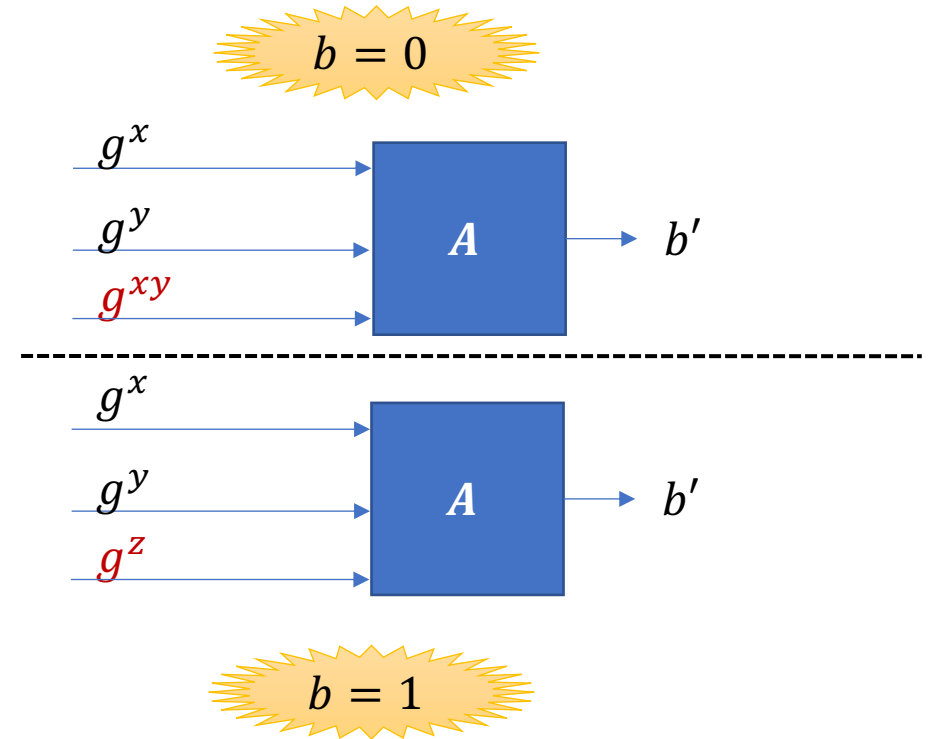
The procedures used in algorithms may sometimes be unspecified (e.g., \mathcal{G}), but parameters should be fully stated.

- Precisely stated computational hardness assumptions.
- Rigorous logical steps from assumptions to conclusion.

THE DECISIONAL DIFFIE-HELLMAN PROBLEM

Experiment:

1. Generate (G, q, g) from \mathcal{G} .
2. Draw random $b \leftarrow \{0,1\}$ and $x, y, z \leftarrow \{1, \dots, t\}$.
3. If $b = 0$, give g^x, g^y, g^{xy} to A ;
4. If $b = 1$, give g^x, g^y, g^z to A ;
5. A returns $b' \in \{0,1\}$.



Definition. The DDH problem is hard relative to \mathcal{G} if, for any PPT A ,

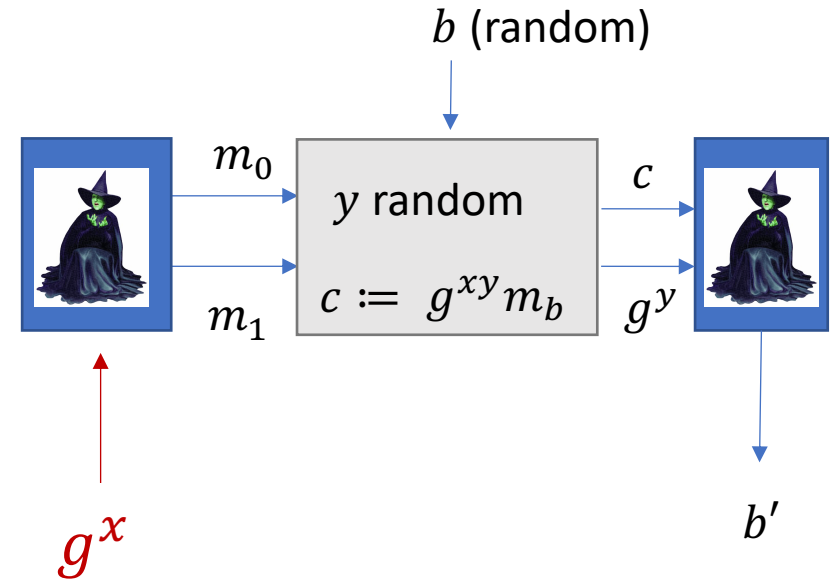
$$| \Pr[A = 1 | b = 0] - \Pr[A = 1 | b = 1] | \leq \text{negl}(n).$$

SECURITY CLAIM

Theorem: If the DDH problem is hard relative to \mathcal{G} , then the El Gamal encryption scheme is IND-CPA secure.

Proof sketch:

We want to prove that Eve has no better than a negligible advantage of guessing b in this experiment.



Experiment E

SECURITY CLAIM

Theorem: If the DDH problem is hard relative to \mathcal{G} , then the El Gamal encryption scheme is IND-CPA secure.

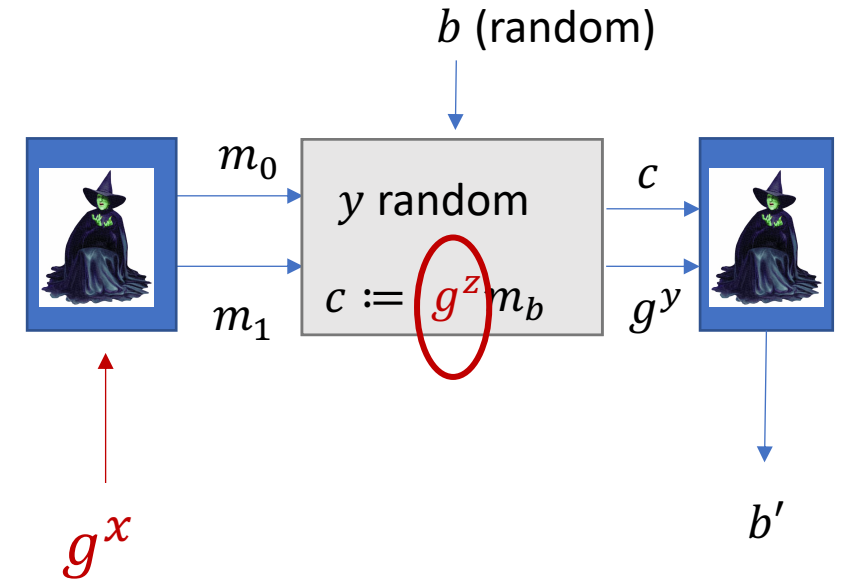
Proof sketch:

We want to prove that Eve has no better than a negligible advantage of guessing b in this experiment.

Suppose we were to modify: replace g^{xy} with a **uniformly random** element g^z .

Eve now gets **no** information at all about b , so her probability of a correct guess is $\frac{1}{2}$.

And by DDH, the outcome of Experiment F is only negligibly different from Experiment E!



Experiment F

RSA ENCRYPTION REVISITED

A QUICK “PRIMER” ON PRIME FACTORIZATION

Every positive integer has a **unique** factorization into primes

$$n = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4} \cdot \dots$$

$$m = 2^{c_1} \cdot 3^{c_2} \cdot 5^{c_3} \cdot 7^{c_4} \cdot \dots$$

Multiplication and exponentiation are easy:

$$nm = 2^{b_1+c_1} \cdot 3^{b_2+c_2} \cdot 5^{b_3+c_3} \cdot 7^{b_4+c_4} \cdot \dots$$

$$n^k = 2^{kb_1} \cdot 3^{kb_2} \cdot 5^{kb_3} \cdot 7^{kb_4} \cdot \dots$$

Exercise: How many factors does $2^3 \cdot 3^4$ have?

Prime factorizations are easy to work with, but sometimes very hard to find!

A QUOTE FROM A MATHEMATICAL ANTI-HERO

“If useful knowledge is [...] knowledge which is likely [...] to contribute to the material comfort of mankind [...] **then the great bulk of higher mathematics is useless.** Modern geometry and algebra, **the theory of numbers**, the theory of aggregates and functions, relativity, quantum mechanics—no one of them stands the test much better than another [...]”

-- G. H. Hardy, *A Mathematician's Apology*, 1940



Source: www.wikipedia.org

Negative predictions are dangerous...

SINGLE-BIT RSA ENCRYPTION



d



N, e



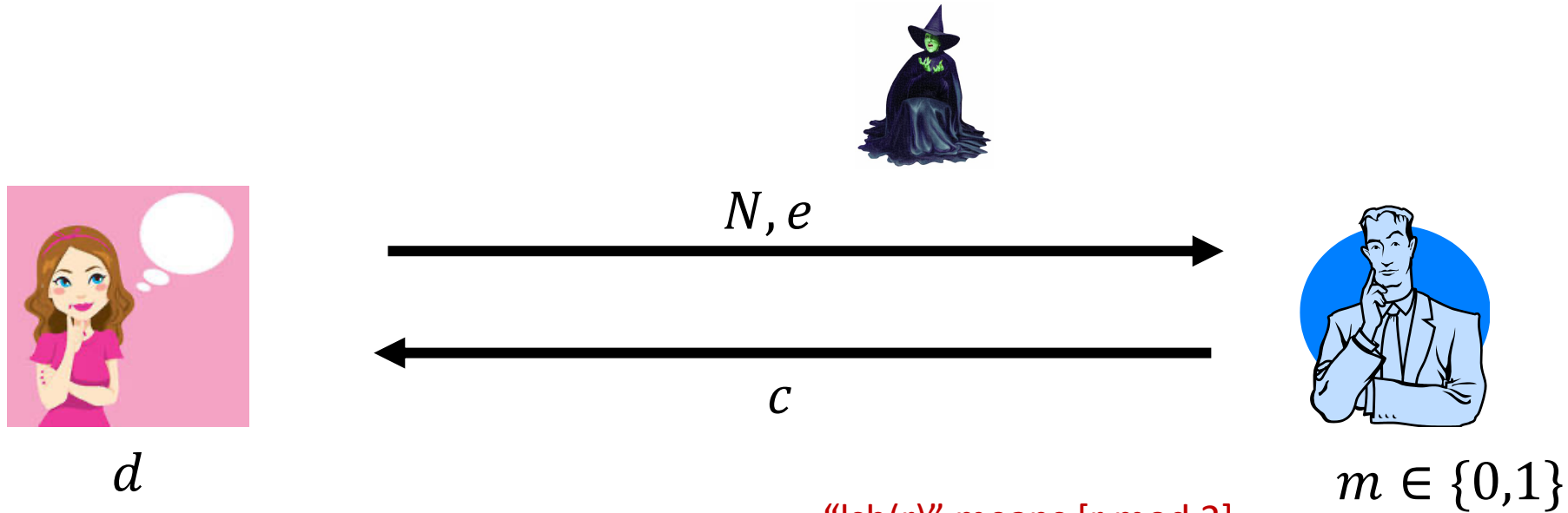
$m \in \{0,1\}$

GenRSA:

Let n = security parameter.

1. Alice generates two random primes p, q of length n , and computes $N=pq$.
2. Alice chooses random $e \in \mathbb{Z}_{(p-1)(q-1)}^*$ and computes its multiplicative inverse (d).

SINGLE-BIT RSA ENCRYPTION



“lsb(r)” means $[r \bmod 2]$.



Enc:

1. Bob chooses random $r \in \mathbb{Z}_N^*$ such that $lsb(r) = m$.
2. He computes $c := [r^e \bmod N]$.

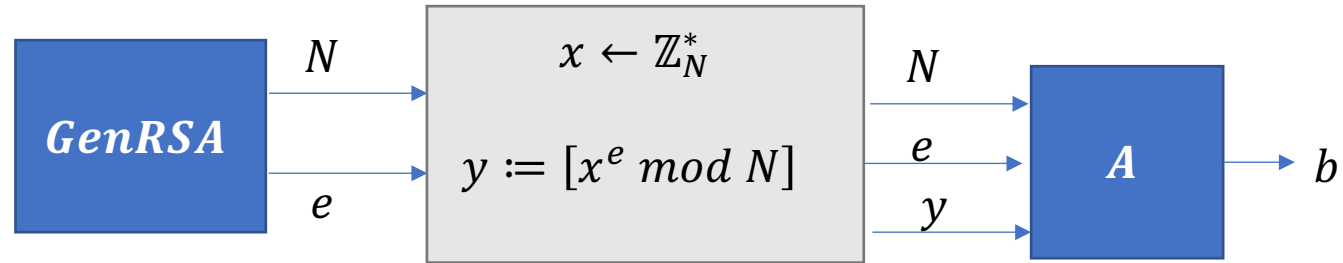
Dec:

1. Alice computes $r = [c^d \bmod N]$, recovers m .

A “HARD-CORE” RSA ASSUMPTION

Experiment:

1. Run GenRSA to obtain N, e .
2. Compute random $x \in \mathbb{Z}_N^*$.
3. Send N, e , and $[x^e \bmod N]$ to A .
4. A outputs bit b .



A wins if $b = \text{lsb}(x)$.

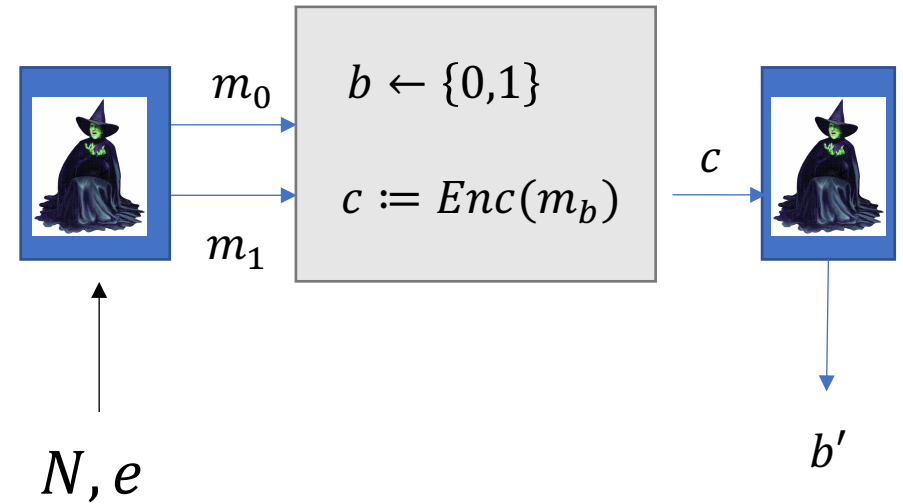
Assumption. The probability that A wins is $\leq \frac{1}{2} + \text{negl}(n)$.

SECURITY CLAIM

Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

Proof sketch:

Consider the IND-CPA experiment. (The bit b is chosen at random.)



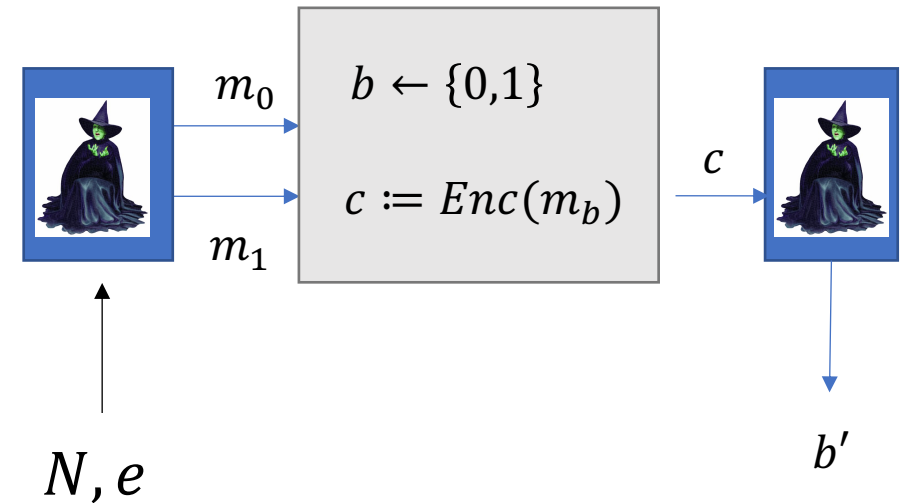
SECURITY CLAIM

Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

Proof sketch:

Consider the IND-CPA experiment. (The bit b is chosen at random.)

Suppose that Eve has a non-neg. advantage.



SECURITY CLAIM

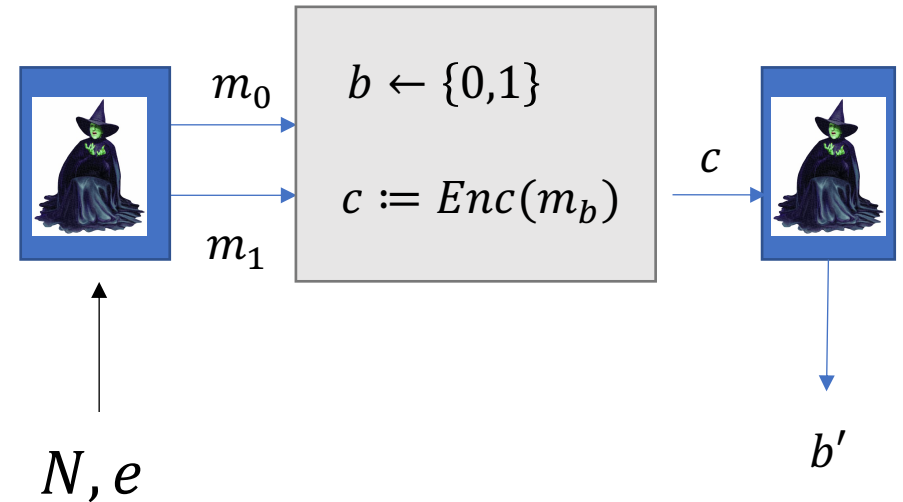
Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

Proof sketch:

Consider the IND-CPA experiment. (The bit b is chosen at random.)

Suppose that Eve has a non-neg. advantage.

We can assume that $m_0 = 0, m_1 = 1$.



SECURITY CLAIM

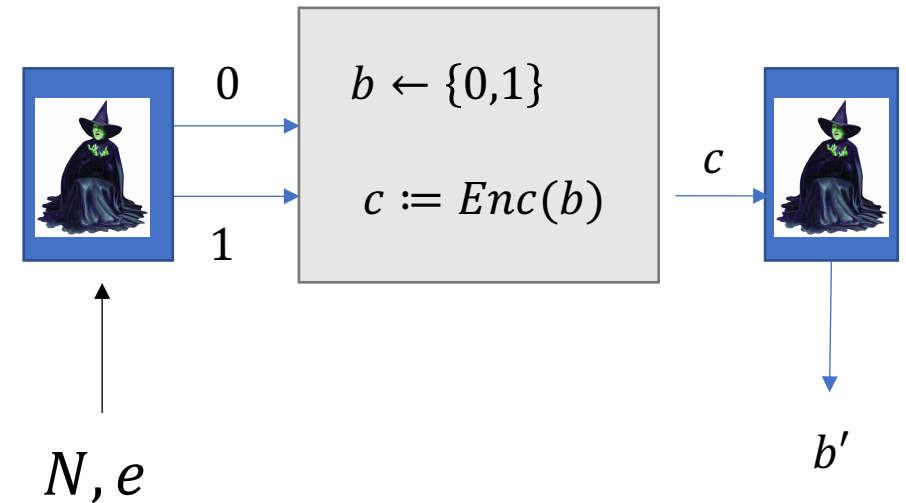
Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

Proof sketch:

Consider the IND-CPA experiment. (The bit b is chosen at random.)

Suppose that Eve has a non-neg. advantage.

We can assume that $m_0 = 0, m_1 = 1$.



SECURITY CLAIM

Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

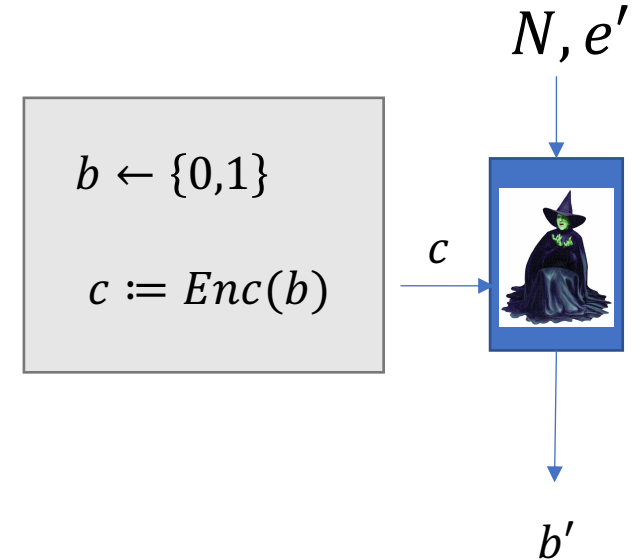
Proof sketch:

Consider the IND-CPA experiment. (The bit b is chosen at random.)

Suppose that Eve has a non-neg. advantage.

We can assume that $m_0 = 0, m_1 = 1$.

The gray box is the same (up to negligible probability) as the one from the hard-core RSA assumption! (With $b := \text{lsb}(x)$.)



SECURITY CLAIM

Theorem: If the hard-core RSA assumption holds, then single-bit RSA is IND-CPA secure.

Proof sketch:

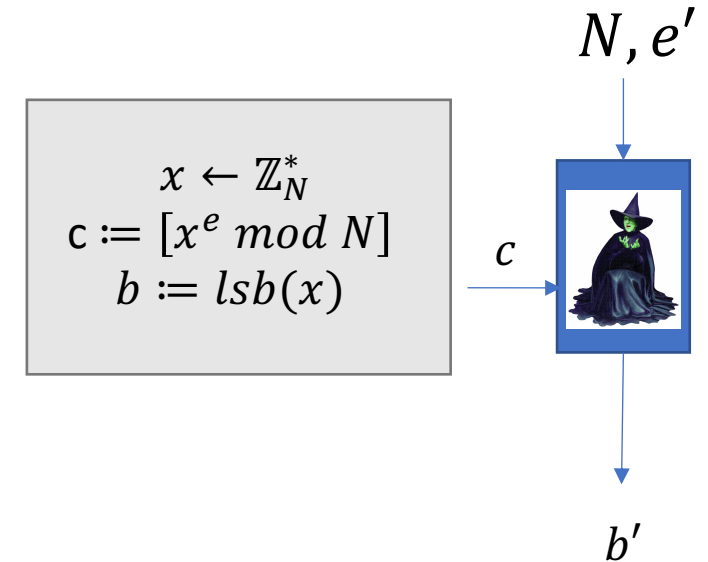
Consider the IND-CPA experiment. (The bit b is chosen at random.)

Suppose that Eve has a non-neg. advantage.

We can assume that $m_0 = 0, m_1 = 1$.

The gray box is the same (up to negligible probability) as the one from the hard-core RSA assumption! (With $b := \text{lsb}(x)$.)

The adversary can achieve a non-negligible advantage at the hard-core RSA experiment. Contradiction.



CONCLUSION

We defined & sketched security proofs for El Gamal and RSA encryption.

In these miniature security proofs, the underlying assumption looks similar to the security claim itself. In longer security proofs, the two claims may look pretty different.

Security proofs are good for judging and comparing different protocols.

EPILOGUE

RSA is one of the most widely used cryptosystems today.

However, it is not the cryptosystem of the future. Why?

EPILOGUE

Digital Computing

Bits



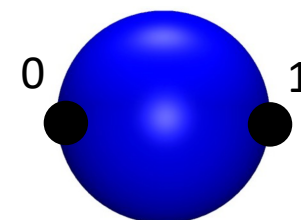
Randomized Computing

**Random
bits**



Quantum Computing

Qubits



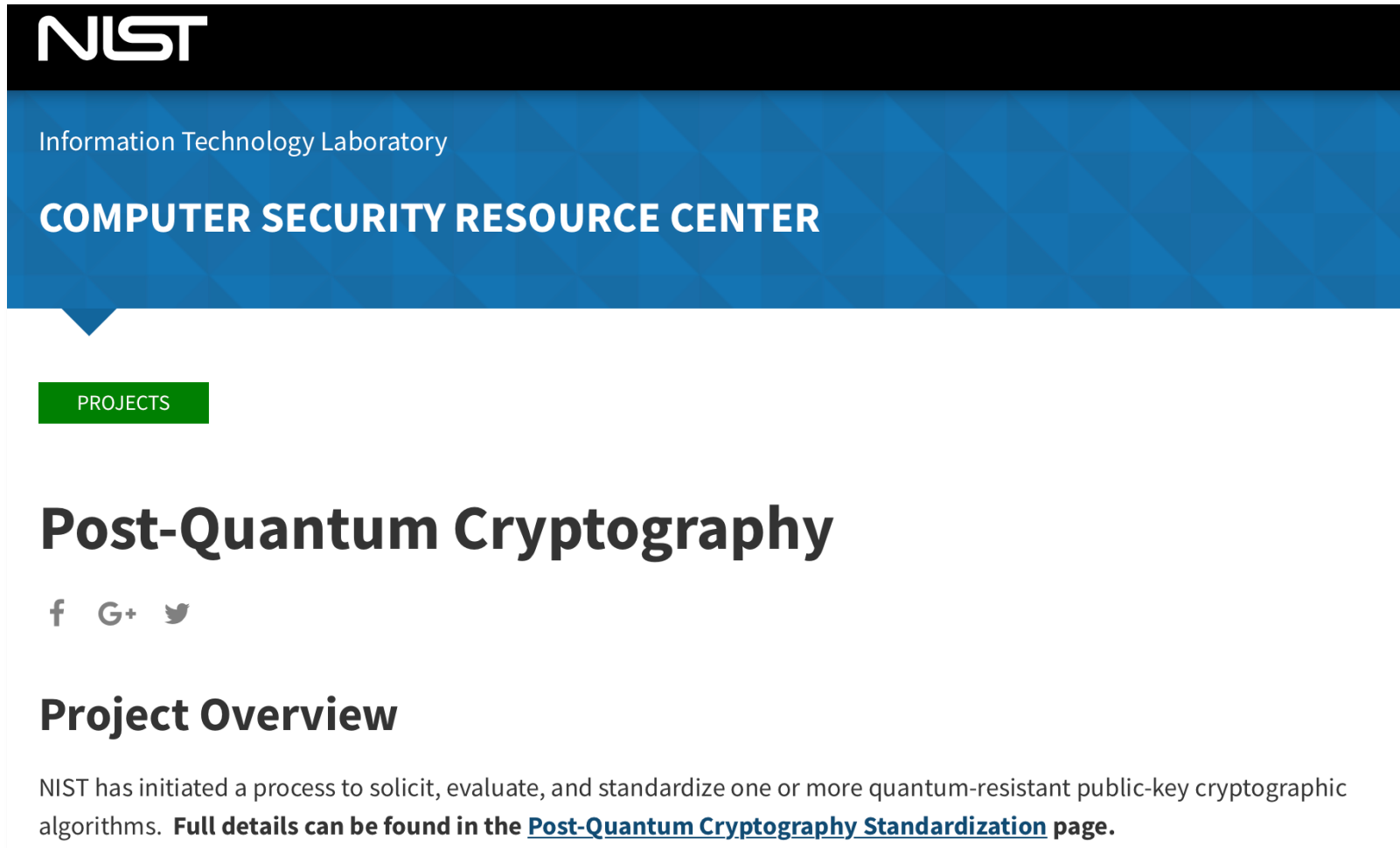
In theory, a quantum computer can factor numbers in polynomial time, breaking RSA. (Shor's algorithm.)

EPILOGUE

“There is strong commercial interest in deploying post-quantum cryptography even before such a quantum computer has been built. Companies and governments cannot afford to have their private communications decrypted in the future, even if that future is 30 years away. For this reason, **there is a need to begin the transition to post-quantum cryptography as soon as possible.**”

-- Quantum Computing: Progress and Prospects

National Academies of Sciences, Engineering, and Medicine



The image shows a screenshot of the NIST Computer Security Resource Center website. At the top left is the NIST logo. Below it, the text 'Information Technology Laboratory' is displayed. The main header area is blue with the text 'COMPUTER SECURITY RESOURCE CENTER' in white. A green button labeled 'PROJECTS' is visible. The main content area features the title 'Post-Quantum Cryptography' in large black font, followed by social media icons for Facebook, Google+, and Twitter. Below this is the section 'Project Overview' with a paragraph of text: 'NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the [Post-Quantum Cryptography Standardization](#) page.'

NIST

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS

Post-Quantum Cryptography

f G+ t

Project Overview

NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the [Post-Quantum Cryptography Standardization](#) page.

NIST is preparing to write “postquantum” cryptographic standards.