Ethics in Cryptography

Adapted from “The Moral Character of Cryptographic Work”
by Phillip Rogaway

Structure and Purpose of This Lecture

Ethics is a subjective topic

Goal of this lecture is *not* to prescribe a certain definition of ethics, but to encourage you to think about what ethics means to you

Structure will be to briefly introduce aspects of cryptography where ethics can play a role, then discussing in small groups and sharing out (if comfortable)

Number one rule: be respectful!

The Ethic of Responsibility

As scientists and engineers, our work often has a large impact on society, whether we plan it to or not

Ethic of Responsibility: one should take this into account by

- Using one's work to contribute to the social good
- Avoiding contributing to social harm

Considering Job offers

How much (if at all) does a “right livelihood” factor into your decisions of what to work on?

Are there fields or specific jobs you would not feel comfortable working in? Any others you might gravitate to?

The ethic of responsibility in decline. And yet, for all I have said, the scientist or engineer seriously concerned about the social impact of his work is, I think, so rare as to be nearly a matter of myth. Never during the cold war, nor in any of the subsequent US wars, did US companies have difficulty recruiting or retaining the hundreds of thousands of scientists and engineers engaged in building weapons systems.[25] Universities like my own were happy to add their support; the University of California would, for decades, run the USA's nuclear weapons design laboratories.[26] In nearly 20 years advising students at my university, I have observed that a wish for *right livelihood*[27] almost never figures into the employment decisions of undergraduate computer science students. And this isn't unique to computer scientists: of the five most highly ranked websites I found on a Google search of *deciding among job offers*, not one suggests considering the institutional goals of the employer or the social worth of what they do.[28]

[Rogaway 2015]

Thoughts From Some Cryptographers

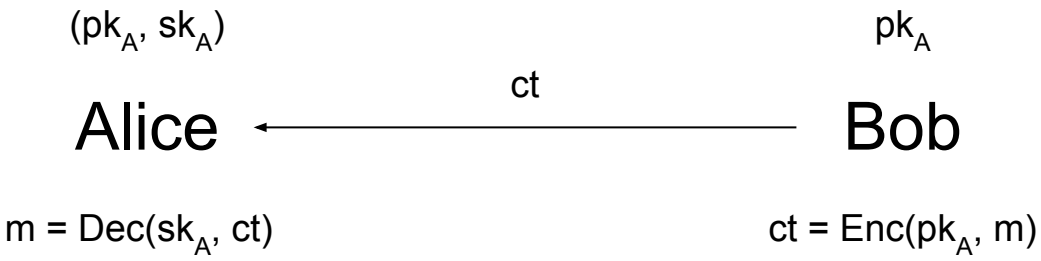
…we were headed into a world where people would have important, intimate, long-term relationships with people they had never met face to face. I was worried about privacy in that world, and that's why I was working on cryptography.

Whitfield Diffie, testimony at the Newegg vs TQP patent trial, 2014

The foundation is being laid for a dossier society, in which computers could be used to infer individuals' life-styles, habits, whereabouts, and associations from data collected in ordinary consumer transactions. Uncertainty about whether data will remain secure against abuse by those maintaining or tapping it can have a 'chilling effect,' causing people to alter their observable activities.

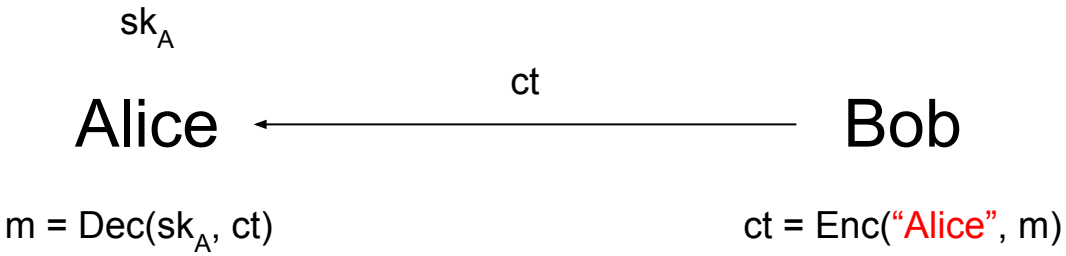
David Chaum, Security without identification: transaction systems to make big brother obsolete

“Standard” Encryption Model



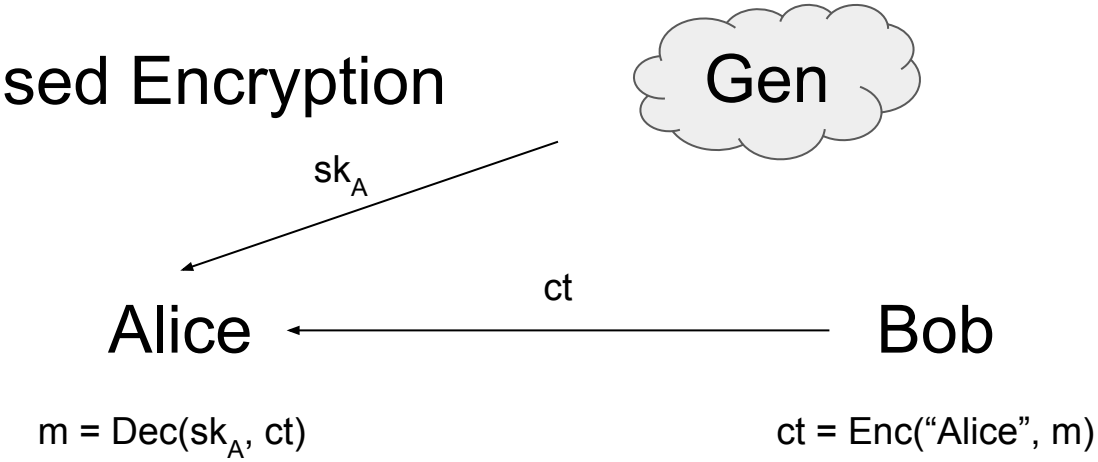
Issue: how does Bob get Alice’s public key?

Identity-Based Encryption



Idea: Alice's "identity" serves as her public key

Identity-Based Encryption



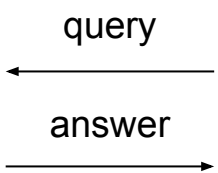
Idea: Alice's "identity" serves as her public key

In order to ensure only Alice has sk_A, need some global key-generation algorithm

Assumption: generation must be trusted–whoever runs it knows everyone's keys!

Differential Privacy

Name	Quest	Fav Color
Alice	Funding	Mint
Bob	Holy Grail	Gold
Charlie	¯_(ツ)_/¯	Fuchsia
…	…	…



Client

≈

Name	Quest	Fav Color
Alice	Funding	Mint
~~Bob~~	~~Holy Grail~~	~~Gold~~
Charlie	¯_(ツ)_/¯	Fuchsia
…	…	…

What assumptions does this model make?

How reasonable / problematic do you feel these assumptions are?

One Perspective [Rogaway 2015]

Focuses on individual privacy only

- This is part of the picture, privacy matters to communities too

Assumes the database controller is trustworthy

- Could be hacked, could use the data for their own purposes, …

Assumes it is ethical to collect large amounts of data in the first place

Privacy Versus Security

“Law Enforcement” Framing

- Privacy as a personal good vs security as a collective good
- The two are in conflict–bad guys use privacy to avoid detection
- A balance is needed between the two, but cryptography and especially encryption breaks that balance

“Surveillance-studies” Framing

- Privacy is also a collective good, and often complements security
- Mass surveillance is an instrument of power, used to stifle dissent while tending to make people uniform and shallow
- Technology makes surveillance much easier–but cryptography can prevent it

Privacy Versus Security Discussion

To what extent do you agree with the “law enforcement” framing / the “surveillance-studies” one? Are there other perspectives neither takes into account?

Given these arguments, would you support or work on stronger encryption? What about weaker encryption or encryption with backdoors? What are the advantages and possible hazards of each of these?

What other areas of computer science could these considerations be relevant to?

Suggestions from [Rogaway 2015]

1) Solve problems with social value, in a way that serves ordinary people
2) Be introspective about why you work on whatever you do
3) Be open to diverse models, and be aware of the drawbacks of each model
4) Think twice about accepting military funding
5) Do research that would frustrate the NSA
6) Learn, use, and improve privacy tools
7) Design and build broadly useful cryptography outside the control of corporations or governments

To what extent do you agree / disagree with these suggestions? Which (if any) might you try to follow?