Announcements

HW9 due Friday (approximation)

Quiz 8 solutions posted on canvas

Upcoming plans:

Wed-Friday: using hardness for crypto (lectures by Noah Stephens-Davidowitz)

Next week: problems even harder than NP-complete

Cryptography I

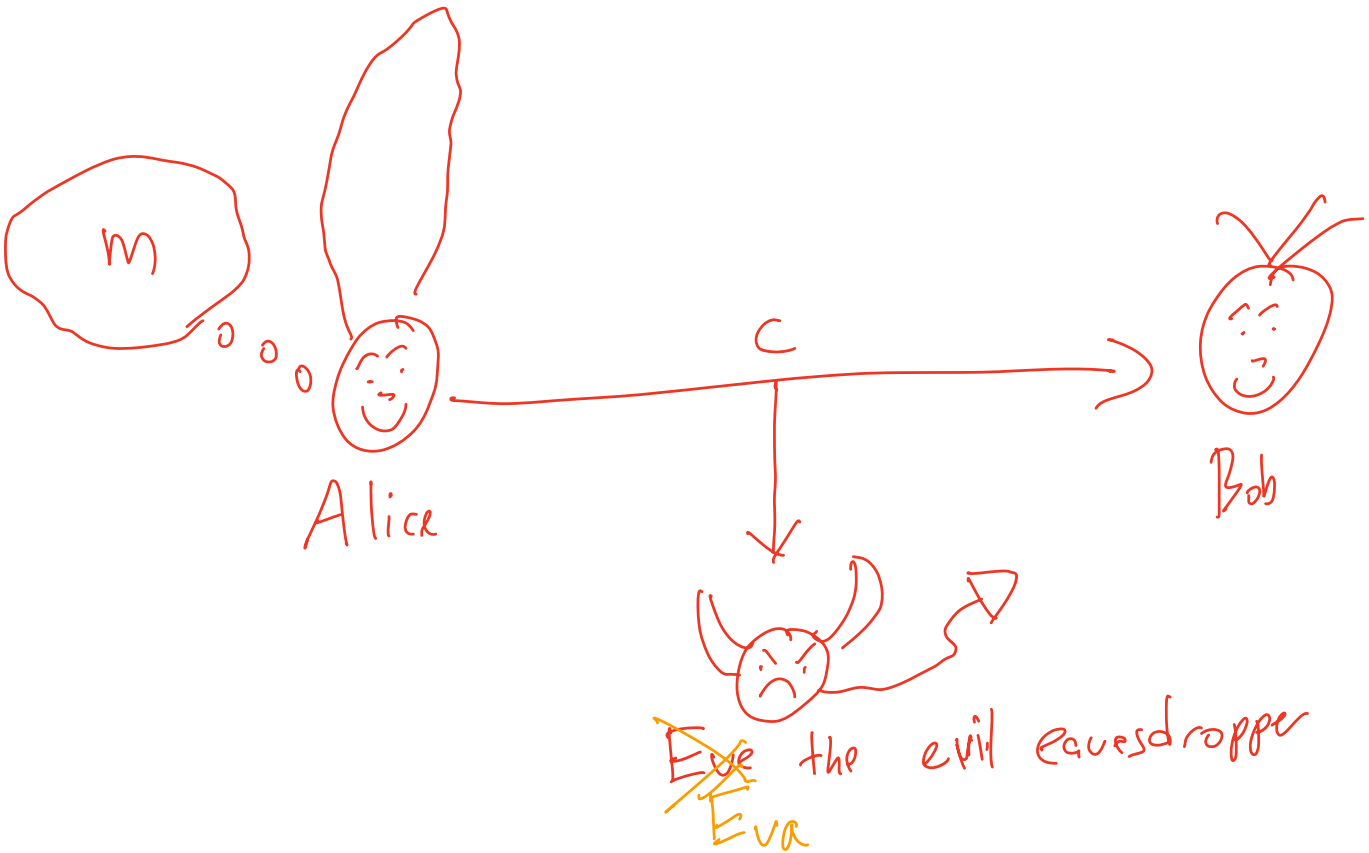
**(See lecture notes for CS4830 at https://www.noahsd.com/crypto_lecture_notes.html .
This is more-or-less Lecture 1 there.)**

Noah Stephens-Davidowitz, April 15, 2026

Cryptography

Sending a message privately

Boring simple idea: $c = m$



Cryptography

Sending a message privately

Cryptography

Sending a message privately

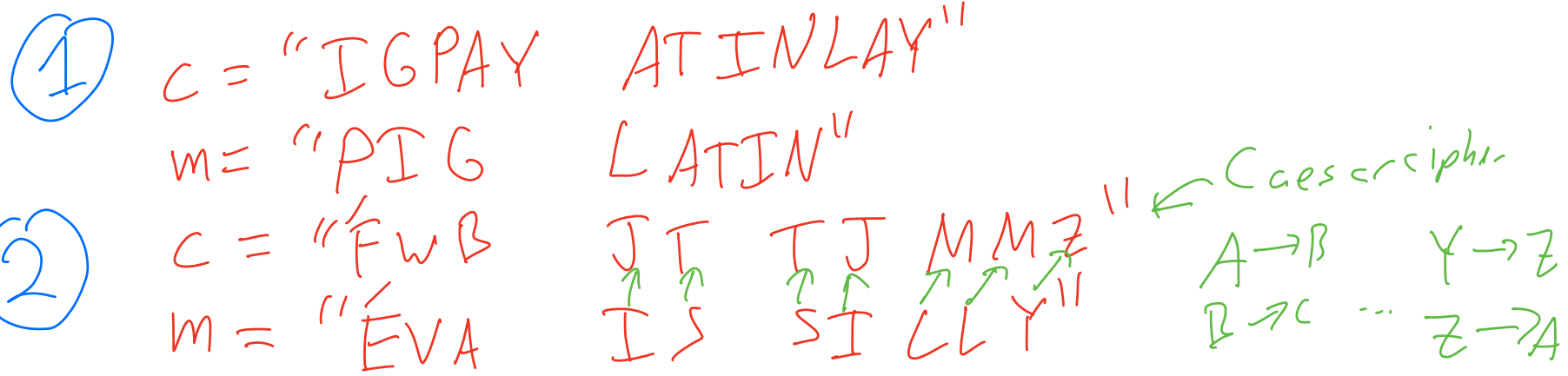
Need a way to encrypt a plaintext m into a ciphertext c, which Bob can decrypt, but “does not reveal m to Éva.”

Cryptography

Sending a message privately

Need a way to encrypt a plaintext m into a ciphertext c, which Bob can decrypt, but "does not reveal m to ~~Eve~~ Éva."

Ad hoc solutions:



Encryption

Sending a message privately

Encryption

Sending a message privately

An encryption scheme consists of a plaintext space M, a ciphertext space C, and a key space K together with **three** algorithms…

Encryption

Sending a message privately

An encryption scheme consists of a plaintext space M, a ciphertext space C, and a key space K together with **three** algorithms…

- An algorithm Gen such that $k \leftarrow \text{Gen}()$ with $k \in K$.

Encryption

Sending a message privately

An encryption scheme consists of a plaintext space M, a ciphertext space C, and a key space K together with **three** algorithms…

- An algorithm Gen such that $k \leftarrow \text{Gen}()$ with $k \in K$.
- An algorithm Enc s.t. if $k \in K, m \in M$, and $c \leftarrow \text{Enc}(k, m)$, then $c \in C$.

Encryption

Sending a message privately

An encryption scheme consists of a plaintext space M, a ciphertext space C, and a key space K together with **three** algorithms…

- An algorithm Gen such that $k \leftarrow \mathsf{Gen}()$ with $k \in K$.
- An algorithm Enc s.t. if $k \in K, m \in M$, and $c \leftarrow \mathsf{Enc}(k, m)$, then $c \in C$.
- An algorithm Dec s.t. if $k \in K, c \in C$, and $m = \mathsf{Dec}(k, c)$, then $m \in M$.

Encryption

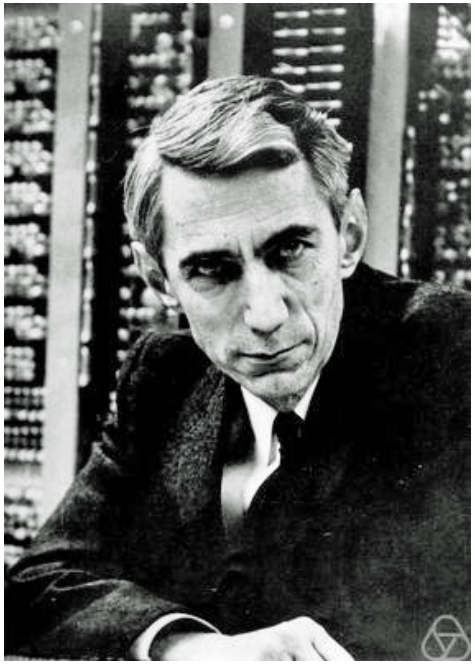
Sending a message privately

An encryption scheme consists of a plaintext space M, a ciphertext space C, and a key space K together with **three** algorithms…

- An algorithm Gen such that $k \leftarrow \text{Gen}()$ with $k \in K$.
- An algorithm Enc s.t. if $k \in K, m \in M$, and $c \leftarrow \text{Enc}(k, m)$, then $c \in C$.
- An algorithm Dec s.t. if $k \in K, c \in C$, and $m = \text{Dec}(k, c)$, then $m \in M$.
- **(Correctness.)** $\forall m \in M, k \in K,$
$$\text{Dec}(k, \text{Enc}(k, m)) = m.$$

Encryption

Perfect indistinguishability [Shannon, 1949]



Claude Shannon

Encryption

Perfect indistinguishability [Shannon, 1949]

Encryption

Perfect indistinguishability [Shannon, 1949]

m_0 = "ÉVA IS SILLY"
m_1 = "ÉVA IS NOT AT ALL SILLY"

Def. An encryption scheme (Gen, Enc, Dec) is perfectly indistinguishable if for any $m_0, m_1 \in M$, and $c \in C$,

$$\Pr_{k \leftarrow \text{Gen}()}[\text{Enc}(k, m_0) = c] = \Pr_{k \leftarrow \text{Gen}()}[\text{Enc}(k, m_1) = c].$$

Encryption

Shannon's one-time pad [Shannon '1949]

$$K = M = C = \{0,1\}^n$$

sampled uniformly

$$\text{Gen}() \sim \{0,1\}^n$$

$$\text{Enc}(k, m) = k \oplus m$$

$$\text{Dec}(k, c) = k \oplus c$$

1100 ⊕ 1001 = 0101

Correctness:

$$\text{Dec}(k, \text{Enc}(k, m)) = k \oplus (k \oplus m) = m$$

Encryption

Shannon's one-time pad [Shannon '1949]

$$K = M = C = \{0,1\}^n$$

$$\text{Gen}() \sim \{0,1\}^n$$

$$\text{Enc}(k, m) = k \oplus m$$

$$\text{Dec}(k, c) = k \oplus c$$

Thm. The one-time pad is perfectly indistinguishable. (I.e., $\forall m_0, m_1, c$

$$\Pr_{k\sim\{0,1\}^n}[\text{Enc}(k, m_0) = c] = \Pr_{k\sim\{0,1\}^n}[\text{Enc}(k, m_1) = c]$$

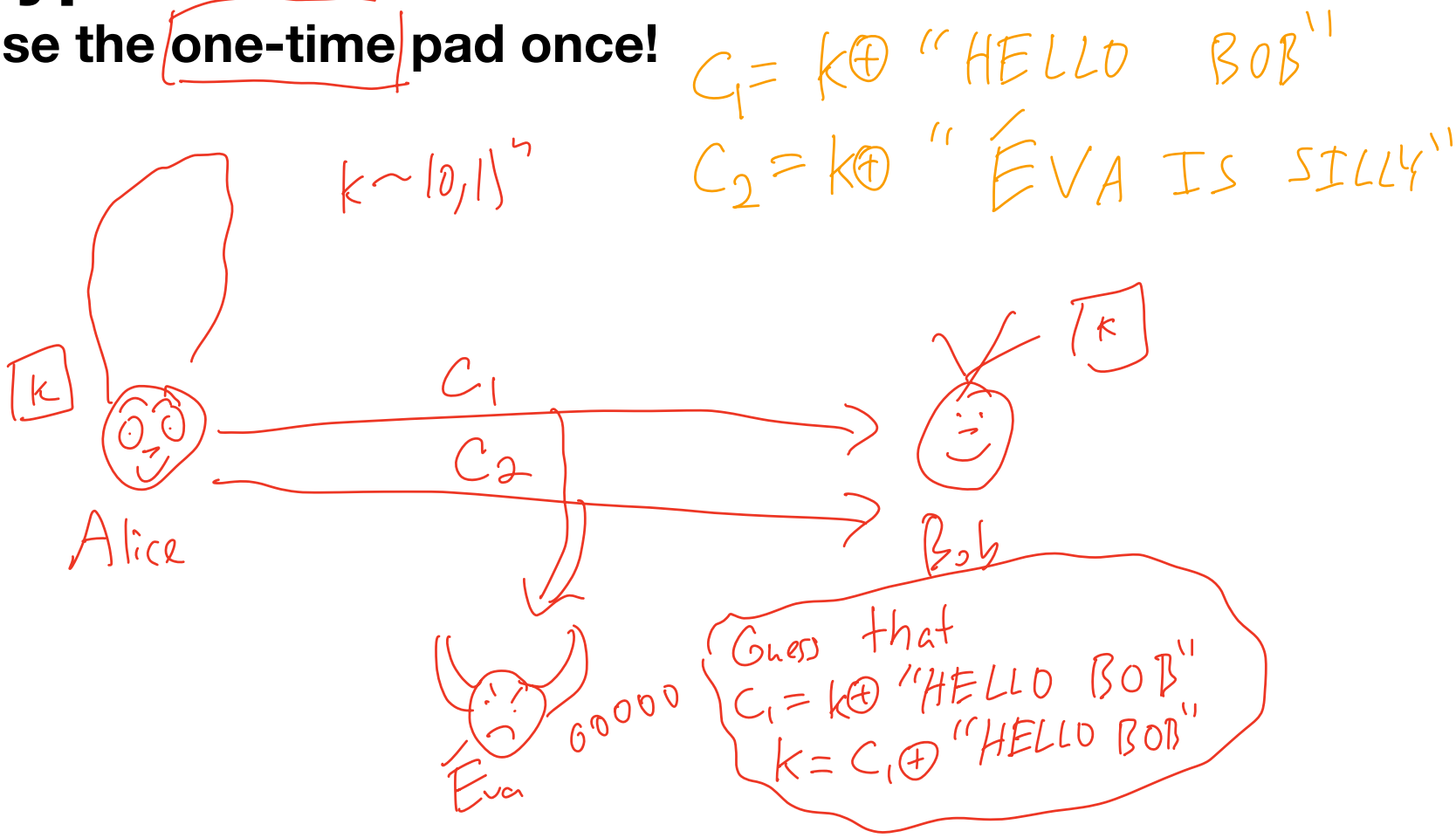
Proof.

$$\Pr_{k\sim\{0,1\}^n}[k \oplus m_0 = c] = \Pr_{k\sim\{0,1\}^n}[k = c \oplus m_0] = 2^{-n}$$

fixed string, uniform

Encryption

Only use the one-time pad once!



Encryption

Only use the one-time pad once!

Thm. If (Gen, Enc, Dec) is a perfectly indistinguishable (and correct) encryption scheme, then $|K| \geq |M|$.

Encryption Éva

How powerful is ~~Eve~~?

Encryption Éva

How powerful is ~~Eve~~?

- Éva is really really smart [citation needed], but even she can’t, for example, brute-force through 2^{256} different secret keys!

Encryption Éva

How powerful is ~~Eve~~?

- Éva is really really smart [citation needed], but even she can't, for example, brute-force through 2^{256} different secret keys!

- Whatever process Éva uses to try to read Alice's messages is itself an algorithm!

Encryption Éva

How powerful is ~~Eve~~?

- Éva is really really smart [citation needed], but even she can't, for example, brute-force through 2^{256} different secret keys!

- Whatever process Éva uses to try to read Alice's messages is itself an algorithm!

- Maybe we can find a way for Alice and Bob to communicate securely *without any shared secret key* in such a way that no **efficient** algorithm can figure out their message.

Cryptography

Fun example: Zero-knowledge proofs