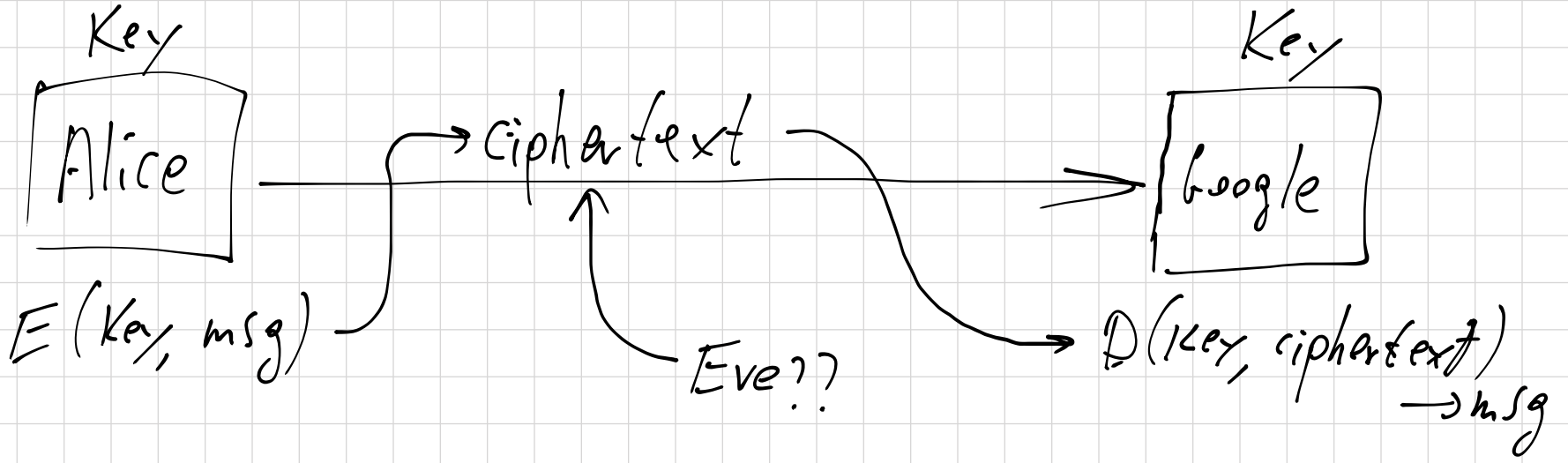
AES GCM (Gunn High school, March 29/30, 2016)

- Today: Tip of crypto ice berg
- Online demo: google.com uses AES-GCM
  Goal: Build it from scratch

What is a cipher? Algs E & D

E(key, msg) → ciphertext

D(key, ciphertext) → message



---

example cipher: one-time pad

message:	H	E	L	L	O	␣	W	O	R	L	D
ASCII:	48	45	4C	4C	4F	20	57	4F	52	4C	44
random key:	21	34	52	71	23	4A	2B	91	B0	57	98
ciphertext:	69	71	9E	BD	72	6A	82	E0	02	A3	E2

⊞ no carry across bytes

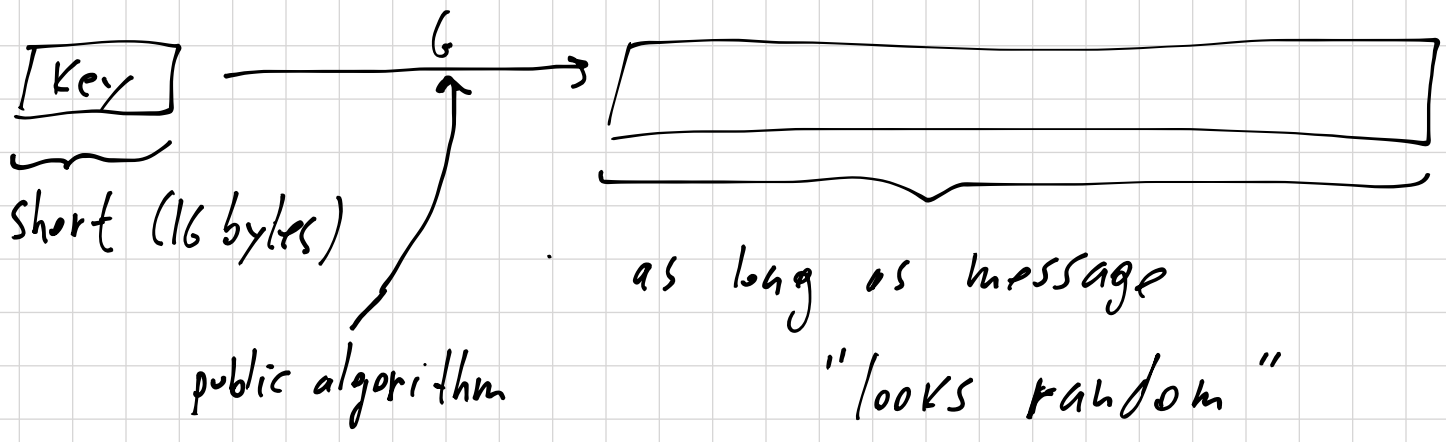
How does decryption work?

Shannon: (1949) IF key is random

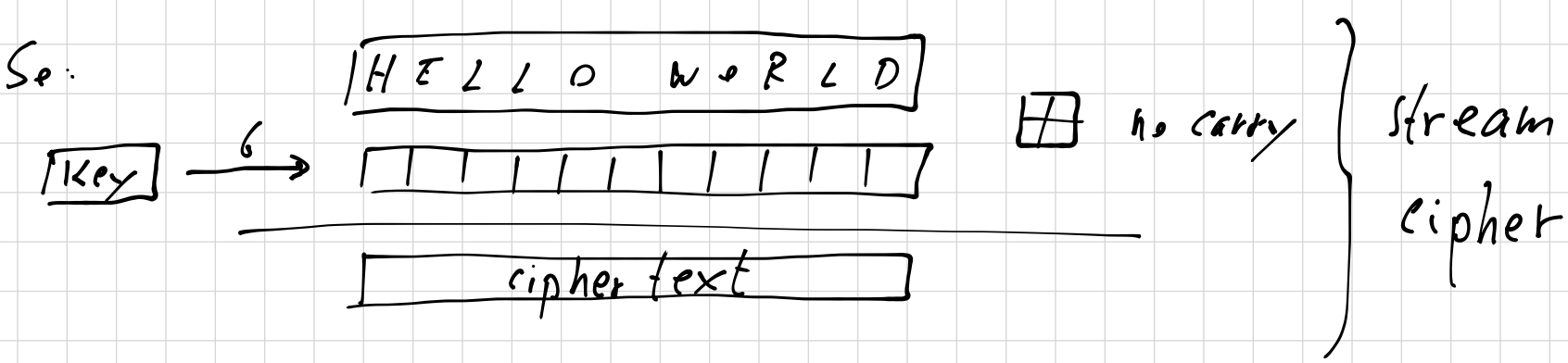
then ciphertext "reveals nothing" about message

Problem: Key is really big !!

Solution: Pseudorandom generator (PRG)



So:



Decryption works by subtraction.

How to build PRG ??

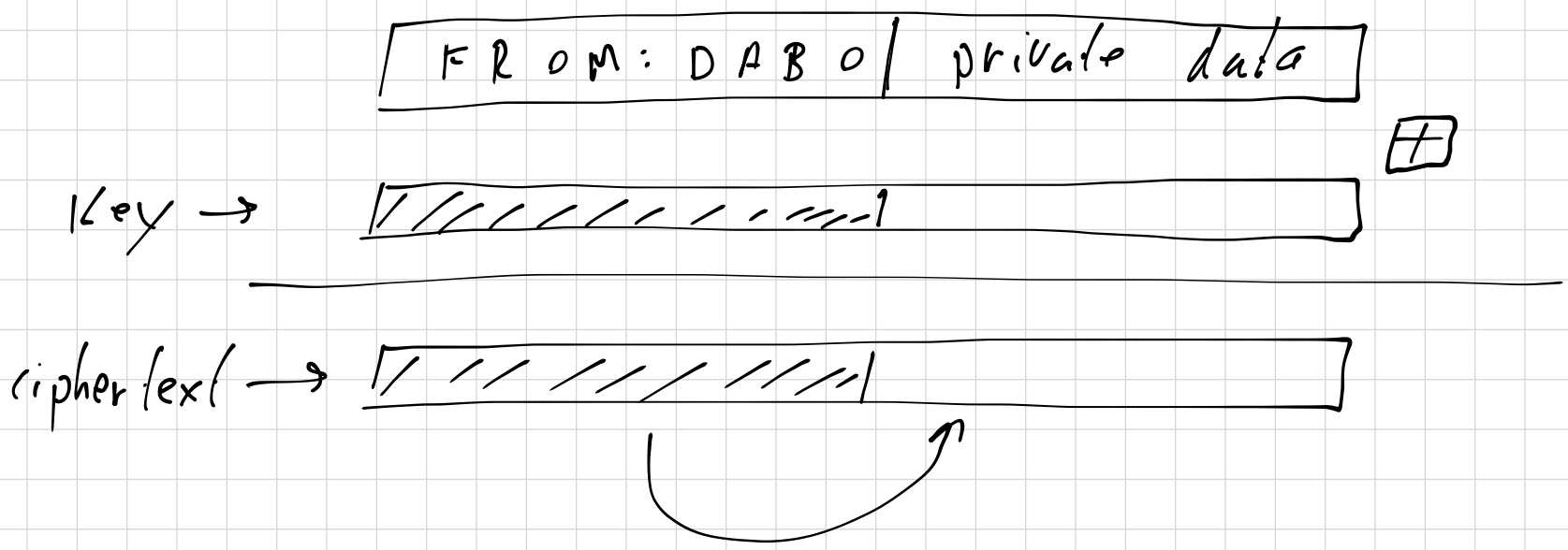
(1) Bad example: G(key) = key | key | key | ... | key

⇒ Show code. They write decryption.
show that using wrong key doesn't decrypt.

Attack 1: letter frequency

Show code ⇒ insecure even though file looks encrypted

Attack 2: known prefix

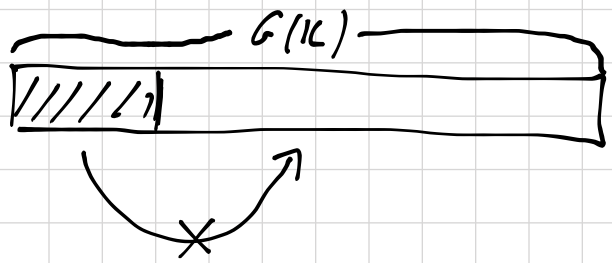


$\Rightarrow$ Given ciphertext and prefix of msg

Eve can recover entire msg.

Property of a secure generator:

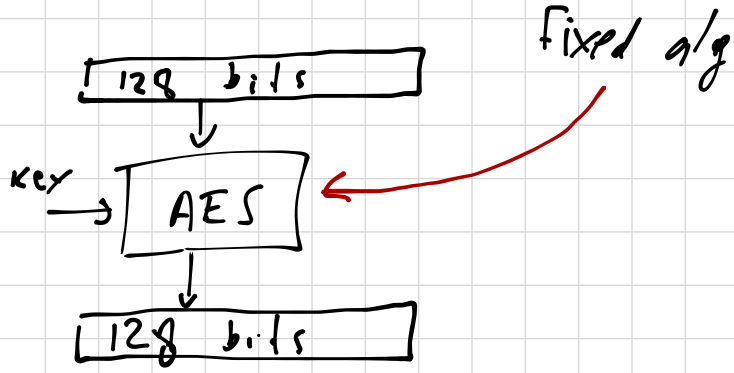
For random key K:



cannot predict from a prefix.

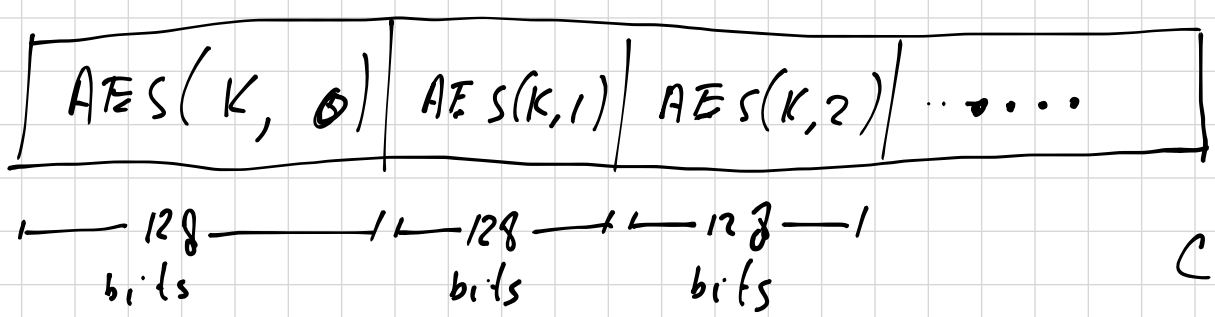
Good generator:

The AES block cipher



Key secret $\Rightarrow$ output always looks random.

PRG(k):



CTR mode

$\Rightarrow$ show code. show that letter freq. attack doesn't work.

Problem: what if we encrypt two files under same key?

m_1 - file #1 , m_2 - file #2

$$\begin{cases} c_1 = E(key, m_1) = m_1 \boxplus F(key) \\ c_2 = E(key, m_2) = m_2 \boxplus F(key) \end{cases}$$

(1) $c_1 = c_2 \Rightarrow m_1 = m_2$

(2) $c_1 - c_2 = m_1 \boxminus m_2$

$\Rightarrow$ enough to recover both messages

Solution: randomness

During encryption chose a random starting point for counter.

$E(key, m)$: 1. choose random 128-bit IV

2. $AES(k, IV) \,||\, AES(k, IV+1) \,||\, AES(k, IV+2) \,||\, \cdots$

ciphertext $\boxplus$ m

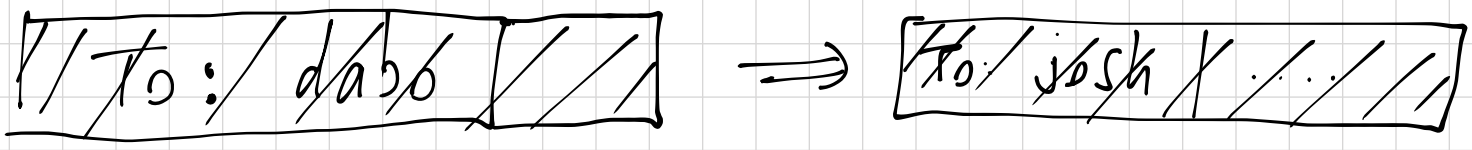
IV

⟹ show code

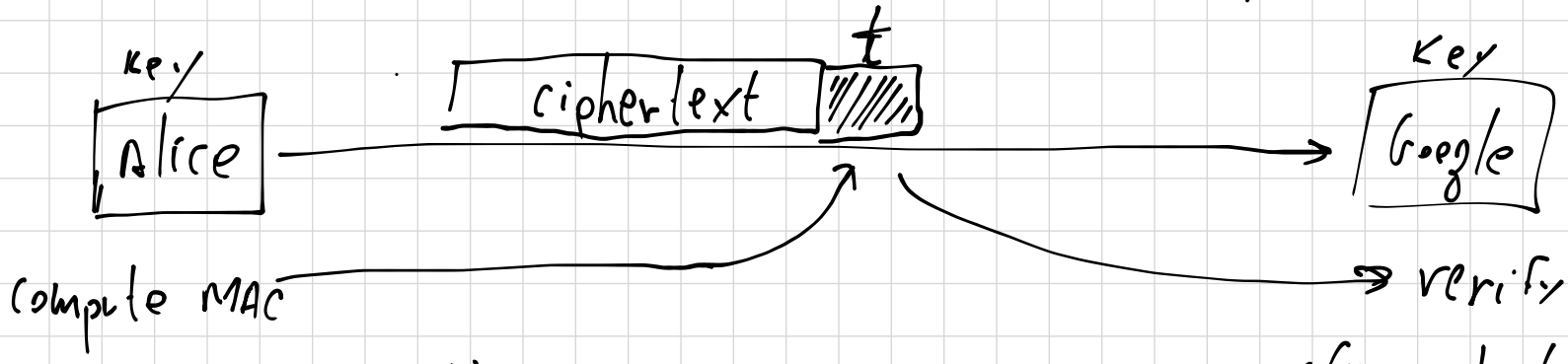
Run twice to show different ciphertexts

Problem: no integrity

⟹ show changing ciphertext w/o detection

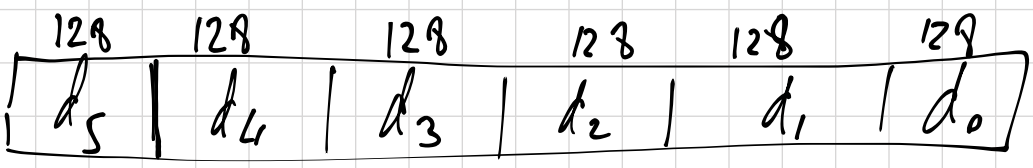


Solution: Message Auth. Code (MAC)



Security: a) attacker sees many valid transmissions,
cannot create a new valid transmission

An example secure MAC: (Carter-Wegman)



$$F(X) = X^6 + d_5 X^5 + d_4 X^4 + \ldots + d_1 X + d_0$$

key = (K, S) two 128-bit values

s(key, data): choose random IV. Set $r \leftarrow AES(k, IV)$

Compute: $t \leftarrow f(s) + r \pmod{2^{128}+51}$

$= s^6 + d_5 s^5 + d_4 s^4 + \dots + d_0 + r \pmod{2^{128}+51}$

output: $[IV, t]$

⇒ show code: show that changing CT results in rejection.

This is a variant of AES-GCM.