Lecture 7

HMAC Revisited:

$$a = H(k \| H(k \| m))$$

(1) Why can't a LEA defeat an HMAC?

* Inner → adversary observes $\langle a, m \rangle$ doesn't see $H(k \| m)$ because of PR of outer hash

* Outer → can extend but you get wrong format:

$$H(k \| H(k \| m) \| z)$$

↳ not $HMAC(m \| z)$

(2) Why can't collisions defeat HMAC?

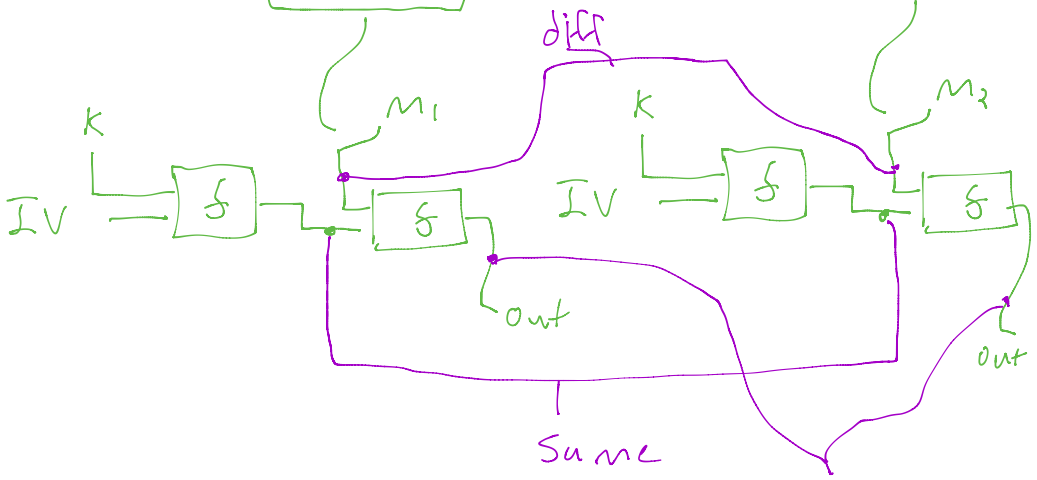
* Given Collision: m_1 and m_2 s.t. $m_1 \neq m_2$

$$H(m_1) = H(m_2)$$

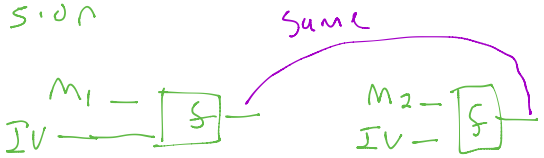
* Question $MAC_k(m_1) \stackrel{?}{=} MAC_k(m_2)$

$MAC_k(m_1) \stackrel{?}{=} MAC_k(m_2)$

$H(k \| H(k \| m_1)) \stackrel{?}{=} H(k \| H(k \| m_2))$



Collision



Composing MACs and Encryption

* This will enable CCA-secure encryption

* This will provide confidentiality & integrity → secure tunnel

① Encrypt-then-MAC (EtM) → SSH

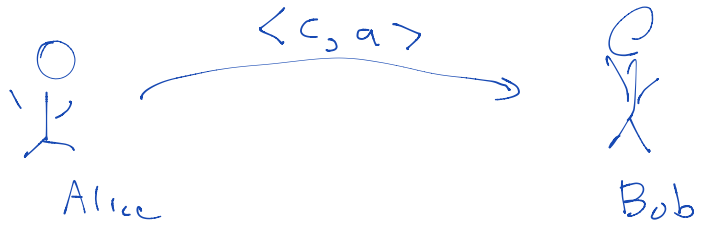
~ CPA-secure

$c = \langle IV , Enc_{K_E}(m \| pad) \rangle$

K_E: encryption/decryption key

$a = MAC_{K_m}(IV, Enc_{K_E}(m \| pad), pad)$

K_m: MAC key.



② MAC-then-Encrypt. → SSL/TLS

$c = \langle IV , Enc_{K_E}(m, MAC_{K_m}(m, pad, IV), pad) \rangle$

③ Authenticated Encryption

↳ combined MAC & CPA-secure

Mode of operation for block ciphers

↳ single pass of message

↳ one common symmetric key.
  ↳ special guarantee.

↳ Example: GCM
  ↳ TLS
  ↳ Counter Mode

↳ Competition to replace GCM
  ↳ CEASER
    ↳ on-going.
      (Dec 2017)

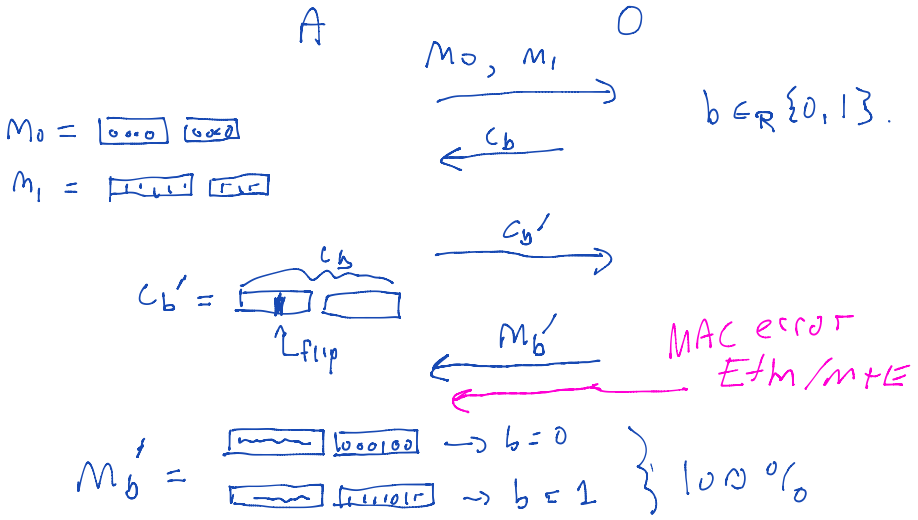
Summary

	OTS	CPA	CCA
ECB	✓	×	×
CBC	✓	✓	×
CTR	✓	✓	×
Stream cipher	✓	✓	×
EtM	✓	✓	✓
MtE	✓	✓	✓
AE/GCM	✓	✓	✓

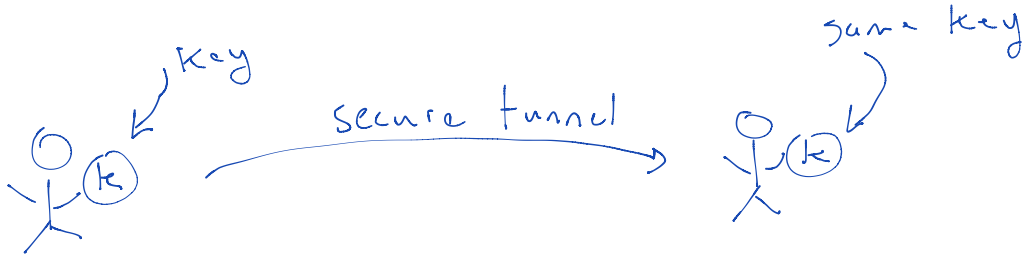
(Same as CTR and Stream cipher)

Intuition for CCA security of EtM/MtE

* Try the CBC/CTR mode attack
* Review.



So far....



Part II: Math-based Cryptography

↳ key agreement

↳ public key / asymmetrical encryption

↳ digital signatures.

Two Mathematical Settings:

* integers from zero to $p-1$ (prime)
  ↳ integers module p
* integers from zero to $n-1$
  ↳ $p \cdot q$ (prime)
  ↳ integers module n.

* Modulus

$a \mod b$

↳ a / b and keep the remainder.

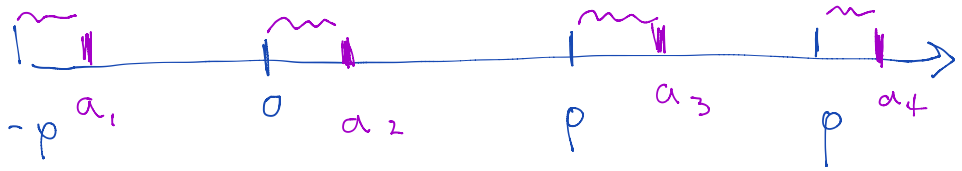
$12 \mod 10 = 2$

$2 \mod 10 \equiv 12$ (congruent.)

* $-8 \equiv 2 \equiv 12 \equiv 22 \equiv 32 \mod 10$

Rule: $(a + x\varphi) \bmod \varphi = a$

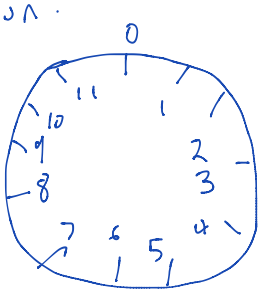
↳ any integer (plus or minus)



$a_1 \equiv a_2 \equiv a_3 \equiv a_4$

Rule: $-a \bmod \varphi = \varphi - a \bmod \varphi$

Application:



↳ integers modulo 12.

10 + 4 hours = 2

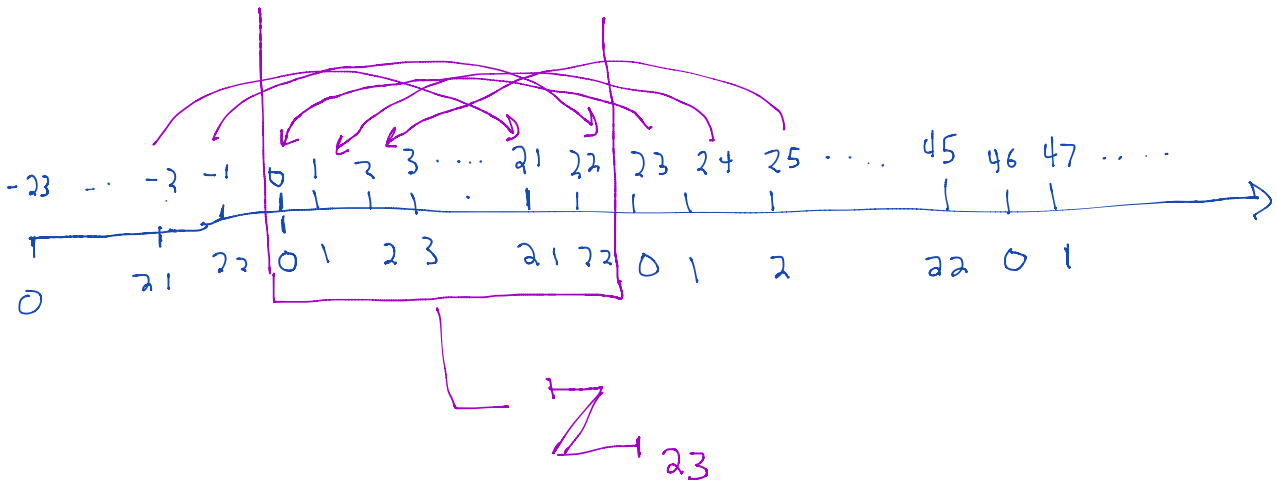
↳ o'clock

↘ $10 + 4 \bmod 12 = 2$

2 o'clock : 4 hours ago.

$$2 - 4 \bmod 12 = -2 \bmod 12$$
$$= +12 - 2 \bmod 12$$
$$= 10$$

Example: mod 23



$\mathbb{Z}_{23}$

↳ set of integers modulo 23.

Groups

* In general a set of integers form a a group: $\mathbb{G}_{q}$ (group, size)

* In a group, integers are not necessarily consequative.

A group consists of:

		This class	In General
(1)	Elements	Integers	Real, Vectors, points, ...
(2)	Operation	Multiplication module p	Addition, xor, point operations, vector addition
(3)	Rules.	See below	

Rules Multiplication module p works like multiplication you are used to.

(1) $a, b \in G \rightarrow a \cdot b \in G$
↳ multiplication module p

(2) $(a \cdot b) \cdot c \rightarrow a \cdot (b \cdot c)$

(3) $\exists e$ s.t. $a \cdot e = a$ ← Identity element
↳ $e = 1$ in our group

④ $\forall a \; \exists b$ s.t. $a \cdot b = 1$

↑ $b = a^{-1}$

⑤ $a \cdot b = b \cdot a$

Want: G_q ← size of group to be prime.

↑ all properties hold ① → ⑤

Is $\mathbb{Z}_p$ a group?

↳ no → zero has no inverse.

↳ drop 0 from $\mathbb{Z}_p$

↳ $\mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$

↳ is a group (✓)

↳ not prime ordered

# of elements.

Fact: $\forall a \in \mathbb{Z}_p^*$ (prime), a is invertible

↳ $\exists b$ s.t. $a \cdot b = 1$

Fact: the order of $\mathbb{Z}_p^*$ is $p-1$

Fact: $p-1$ is never prime (except $p=3$)
↑ prime

($p-1$ is always even and therefore $\frac{p-1}{2}$ is always an integer)

Multiplication mod 23

inverses.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
2	2	4	6	8	10	12	14	16	18	20	22	1	3	5	7	9	11	13	15	17	19	21
3	3	6	9	12	15	18	21	1	4	7	10	13	16	19	22	2	5	8	11	14	17	20
4	4	8	12	16	20	1	5	9	13	17	21	2	6	10	14	18	22	3	7	11	15	19
5	5	10	15	20	2	7	12	17	22	4	9	14	19	1	6	11	16	21	3	8	13	18
6	6	12	18	1	7	13	19	2	8	14	20	3	9	15	21	4	10	16	22	5	11	17
7	7	14	21	5	12	19	3	10	17	1	8	15	22	6	13	20	4	11	18	2	9	16
8	8	16	1	9	17	2	10	18	3	11	19	4	12	20	5	13	21	6	14	22	7	15
9	9	18	4	13	22	8	17	3	12	21	7	16	2	11	20	6	15	1	10	19	5	14
10	10	20	7	17	4	14	1	11	21	8	18	5	15	2	12	22	9	19	6	16	3	13
11	11	22	10	21	9	20	8	19	7	18	6	17	5	16	4	15	3	14	2	13	1	12
12	12	1	13	2	14	3	15	4	16	5	17	6	18	7	19	8	20	9	21	10	22	11
13	13	3	16	6	19	9	22	12	2	15	5	18	8	21	11	1	14	4	17	7	20	10
14	14	5	19	10	1	15	6	20	11	2	16	7	21	12	3	17	8	22	13	4	18	9
15	15	7	22	14	6	21	13	5	20	12	4	19	11	3	18	10	2	17	9	1	16	8
16	16	9	2	18	11	4	20	13	6	22	15	8	1	17	10	3	19	12	5	21	14	7
17	17	11	5	22	16	10	4	21	15	9	3	20	14	8	2	19	13	7	1	18	12	6
18	18	13	8	3	21	16	11	6	1	19	14	9	4	22	17	12	7	2	20	15	10	5
19	19	15	11	7	3	22	18	14	10	6	2	21	17	13	9	5	1	20	16	12	8	4
20	20	17	14	11	8	5	2	22	19	16	13	10	7	4	1	21	18	15	12	9	6	3
21	21	19	17	15	13	11	9	7	5	3	1	22	20	18	16	14	12	10	8	6	4	2
22	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

$5^3 = 10$

$125 \bmod 23 = 10$