TOPIC: 6.857

DATE: 3/9/16

FILE UNDER:

PAGE: L11.1

Admin:

(final projects!)

Today:

Message Authentication Codes (MACs)

- HMAC
- CBC-MAC
- PRF-MAC
- One-time MAC (problem stmt)

AEAD (Authenticated Encryption with Associated Data)

- EAX mode
- Encrypt-then-MAC

Finite fields & # theory

Readings:

Katz: Chapter 4, Chapter 7 (7.1-7.3)

Paar: Ch. 12, Ch. 6.3

TOPIC:

DATE:

FILE UNDER:

PAGE: L12.2

MAC (Message Authentication Code)

- Not confidentiality, but integrity (recall "CIA")
- Alice wants to send messages to Bob, such that Bob can verify that messages originated with Alice & arrive unmodified.
- Alice & Bob share a secret key K
- Orthogonal to confidentiality; typically do both (e.g. encrypt, then append MAC for integrity)
- Need additional methods (e.g. counters) to protect against replay attacks

$$\underset{\substack{M \\ K}}{\text{Alice}} \xrightarrow{\quad M,\ MAC_K(M) \quad} \underset{K}{\text{Bob}}$$

[Here M is message to be authenticated, which could be ciphertext resulting from encryption.]

- Alice computes $MAC_K(M)$ & appends it to M.
- Bob recomputes $MAC_K(M)$ & verifies it agrees which what is received. If $\neq$, reject message.

If MAC has t bits, then Adv has prob 2^{-t} of successful forgery.
Good MAC is (keyed) PRF.

Adversary (Eve) wants to forge $M', MAC_K(M')$ pair that Bob accepts, without Eve knowing K.

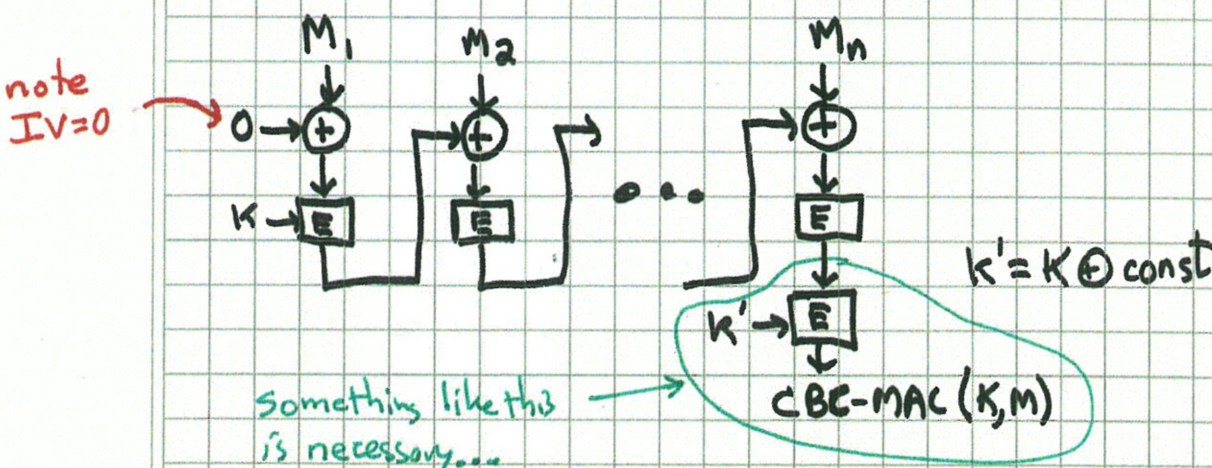
- She may hear a number of valid $(M, MAC_K(M))$ pairs first, possibly even with M's of her choice (chosen msg attacks).
- She wants to forge for M' for which she hasn't seen $(M', MAC_K(M'))$ valid pair.

Two common methods:

HMAC $(K, M) = h(K_1 \| h(K_2 \| M))$

where $K_1 = K \oplus opad$, $K_2 = K \oplus ipad$ — opad, ipad are fixed constants

CBC-MAC $(K, M) \cong$ last block of CBC enc. of M



TOPIC:

DATE:

FILE UNDER:

MAC using random oracle (PRF):

OK for $h = RO$
can be bad for $h =$ iterative hash fn

$$MAC_K(M) = h(K \| M)$$

(OK if h is indistinguishable from RO, which means, as we saw, for sequential hash fns, that last block may need special treatment.)

One-Time MAC (problem stmt):

Can we achieve security against <u>unbounded</u> Eve, as we did for confidentiality with OTP, except here for integrity?

Here key K may be "use-once" [as it was for OTP].

$$\underset{K}{A} \xrightarrow{\quad M,T \quad} \underset{K}{B}$$

$T = MAC_K(M)$ ("tag")

- Eve can learn M,T then try to replace M,T with M',T' (where $M' \neq M$) that Bob accepts.
- Eve is computationally <u>unbounded</u>.

TOPIC:

DATE:

FILE UNDER:

PAGE: L12.5

	Confidentiality	Integrity
Unconditional	OTP ✓	One-time MAC ?
Conventional (symmetric key)	Block ciphers (AES) ✓	MAC (HMAC) ✓
Public-key (asymmetric)	PK enc.	Digital signature

Note: digital signature are unforgeable, but also have nonrepudiation, since only one copy of signing key exists.

TOPIC: 6.857

DATE: 3/11/13

FILE UNDER:

PAGE:

Authenticated Encryption

- EAX mode

[See pgs 1-10 of

The EAX Mode of Operation

by Bellare, Rogaway, & Wagner

]

Figure 3

- Encrypt-then-MAC

$C = \mathrm{Enc}(K_1, M)$

$T = \mathrm{MAC}(K_2, H \| C)$ ← C, not M!

↑ header

{not encrypted, but authenticated

xmit: H, C, T

Two passes

Two keys

TOPIC:

FILE UNDER:

DATE:

Finite fields:

System $(S, +, \cdot)$ s.t.

- S is a finite set containing "0" & "1"
- $(S, +)$ is an abelian (commutative) group with identity 0

group laws
$$\left[\begin{array}{ll} ((a+b)+c) = (a+(b+c)) & \text{associative} \\ a+0 = 0+a = a & \text{identity } 0 \\ (\forall a)(\exists b)\ a+b=0 & \text{(additive) inverses } b=-a \end{array}\right.$$

$a+b = b+a$ commutative

- $(S^*, \cdot)$ is an abelian group with identity 1

S^* = nonzero elements of S

group laws
$$\left[\begin{array}{ll} (a\cdot b)\cdot c = a\cdot(b\cdot c) & \text{associative} \\ a\cdot 1 = 1\cdot a = a & \text{identity } 1 \\ (\forall a \in S^*)(\exists b \in S^*)\ a\cdot b = 1 & \text{(multiplicative inverses) } b = a^{-1} \end{array}\right.$$

$a\cdot b = b\cdot a$ commutative

- Distributive laws: $a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a$ (follows)

Familiar fields: $\mathbb{R}$ (reals) are infinite

$\mathbb{C}$ (complex)

For crypto, we're usually interested in finite fields,

such as Z_p (integers mod prime p)

TOPIC:

DATE:

FILE UNDER:

Over field, usual algorithms work (mostly).

E.g. solving linear eqns:

$$ax + b = 0 \pmod p$$

$$\Rightarrow \quad x = a^{-1} \cdot (-b) \pmod p \quad \text{is soln.}$$

$$3x + 5 = 6 \pmod 7$$

$$3x = 1 \pmod 7$$

$$x = 5 \pmod 7$$

Notation: $GF(q)$ is *the* finite field ("Galois field") with q elements

Theorem: $GF(q)$ exists whenever

$$q = p^k, \ p \text{ prime}, \ k \geq 1$$

Two cases:

① $GF(p)$ - work modulo prime p

$\mathbb{Z}_p$ = integers mod p = $\{0, 1, \ldots, p-1\}$

$\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\} = \{1, 2, \ldots, p-1\}$

② $GF(p^k)$: $k > 1$

work with polynomials of degree $< k$
with coefficients from $GF(p)$
modulo fixed irreducible polynomial of degree k

Common case is $GF(2^k)$

Note: all operations can be performed efficiently

(inverses to be demonstrated)

TOPIC:

DATE:

FILE UNDER:

PAGE:

Construction of $GF(2^2) = GF(4)$

Has 4 elements.

Is <u>not</u> arithmetic mod 4. (where 2 has no mult. inverse)

elements are polynomials of ~~degree~~ degree < 2 with coefficients
mod 2 (i.e. in $GF(2)$):

0
1
x
$x+1$

Addition is component-wise according to powers, as usual

$$(x) + (x+1) = (2x+1) = 1 \quad (\text{coefs. mod } 2)$$

Multiplication is modulo x^2+x+1
which is <u>irreducible</u> (doesn't factor)

	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \bmod (x^2+x+1)$ is $x+1$ (note that $x \equiv -x$ coefs mod 2)