SHA-3

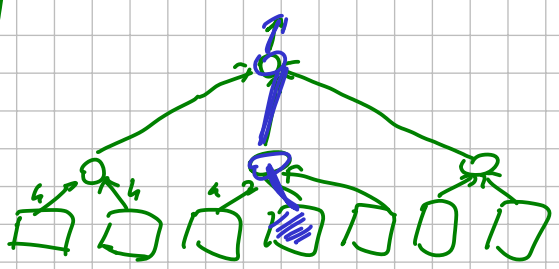
Sponge based on Keccak
↓
perm. on 1600-bit blocks
$n = 1600$

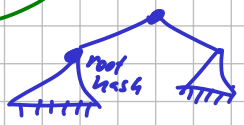
always: $c = 2 \cdot$ out length

hash funcs.	r	c
SHA3-224	1152	448
⋮		
SHA3-512	576	1024
SHAKE-128	1344	256
SHAKE-256	1088	512

XOF
Extensible-Output Functions

Merkle Tree





add a bit "I am root"
→ Sakura coding

MACs (Message Authentication Codes)

usually:
sign deterministic (exc. for N)
verify = sign + compare

Security model (CPA)

Attacker has access to signing oracle
- asks oracle to sign $x_1 \dots x_N$
- produced (forged) signature for message x diff. from all x_i's

Example: $h(K \| X)$ is secure for random h
but not for Merkle-Damgård hashes!
$h(K \| X \| x')$ from $h(K \| X)$ and x'
don't use with SHA-1/2

for SHA-3 OK, called KMAC

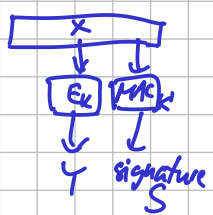
Or: $h(X \| K)$

$HMAC_h(X, K) := h(K \oplus c_{out} \| h(K \oplus c_{in} \| X))$

believed to be OK even with SHA-1

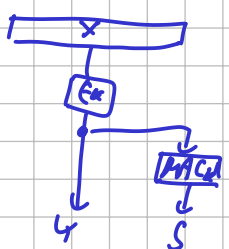
Combining authentication with encryption?

① encrypt & MAC



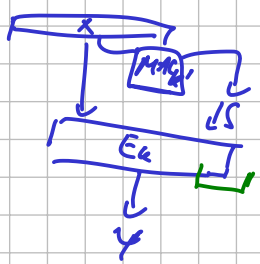
leaks info!

② encrypt, then MAC



recommended

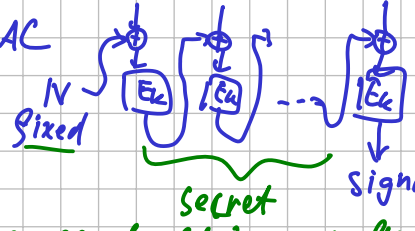
③ MAC, then encrypt



→ has a padding oracle! (by timing)
↓ decrypt

TLS v1.2 (most HTTPS)

CBC-MAC



Has security proof for:
- ideal cipher
- fixed IV
- prefix-free set of msgs

no message should be a prefix of another!
↳ start msg with length

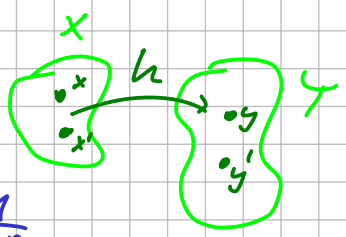
Shannon-secure MACs

single-use random keys $sign(x,k)$

Def: Given a known pair $(x, sign(x))$ all signatures of $x' \neq x$ are equally probable.] for random key

Construction

Def: A set of functions from X to Y
$\mathcal{H} := \{ h_k \mid k \in \mathcal{K} \}$
is 2-independent iff
$\forall_{\substack{x,x' \in X \\ x \neq x'}} \; \forall_{y,y' \in Y} \; Pr_{h \in \mathcal{H}}[h(x)=y \;\&\; h(x')=y'] = \frac{1}{|Y|^2}$



Example: $X, Y = GF(m)$ $\mathcal{K} = GF(m)^2$
$h_{a,b}(x) := ax + b$
is 2-indep. $Pr_{a,b}[\, ax+b=y \;\&\; ax'+b=y' \,] = \frac{1}{|Y|^2}$
has unique solution

2-ind. → MAC Select $h \in \mathcal{H}$ at random
Key = h (params of)
Signature = $h(x)$

$Pr_k[h_k(x')=y' \mid h_k(x)=y] = \frac{Pr_h[h(x)=y \;\&\; h(x')=y']}{Pr_h[h(x)=y]}$ ← by 2-independence of $\mathcal{H}$ this is $1/|Y|^2$

$= \frac{1/|Y|^2}{1/|Y|} = \frac{1}{|Y|}$.

$\sum_{y'} Pr_h[h(x)=y \;\&\; h(x')=y'] = \frac{|Y|}{|Y|^2} = \frac{1}{|Y|}$ ($1/|Y|^2$ each)

Polynomial-based MAC

field F $X = F^n$ $Y = F$ $K = F^2$

$h_{a,b}(x_1 \ldots x_n) := x_1 a^n + x_2 a^{n-1} + \ldots + x_n a^1 + b$

compute in $O(n)$ by Horner's rule

$Pr_{a,b}[h_{a,b}(x'_1 \ldots x'_n) = y' \mid h_{a,b}(x_1 \ldots x_n) = y] =$

$\frac{Pr[\text{left} \;\&\; \text{right}]}{Pr[\text{right}]} \leq \frac{n/|F|^2}{|F|/|F|^2} = \frac{1}{|F|} \Big\} \leq \frac{n}{|F|}$

$Pr_{a,b}[\, (x'_1 a^n + \ldots + x'_n a^1 + b = y') \;\&\; (x_1 a^n + \ldots + x_n a^1 + b = y) \,]$

$(x'_1 - x_1)a^n + \ldots + (x'_n - x_n)a^1 = y' - y$
⇒ at most n values of a
exactly one value of b
} at most n pairs (a,b)

Next weeks: turn these to practical MACs
random generators
... number theory ...