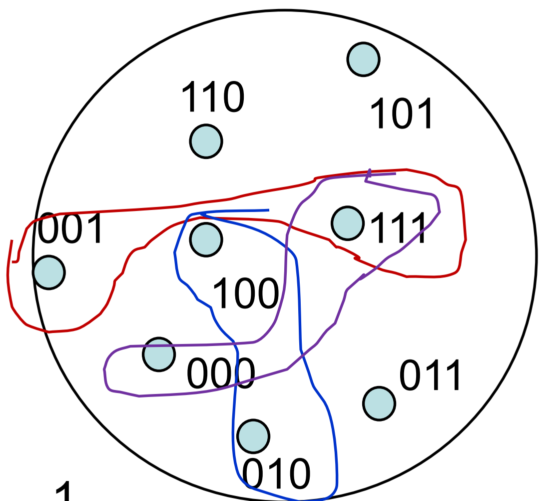
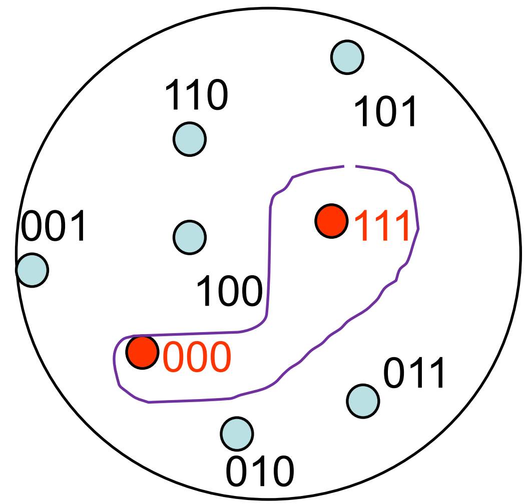
A-code/E-code

Message source M= {0,1}



	0	1
K1	01	11
K2	10	00
K3	00	11
K4	01	10
K5	00	01
K6	11	01
K7	11	10

Authentication code is a subset of the whole space *for each key.*



Error correcting code is a subset of the whole space.

Security

- Success probability of the adversary in forgery

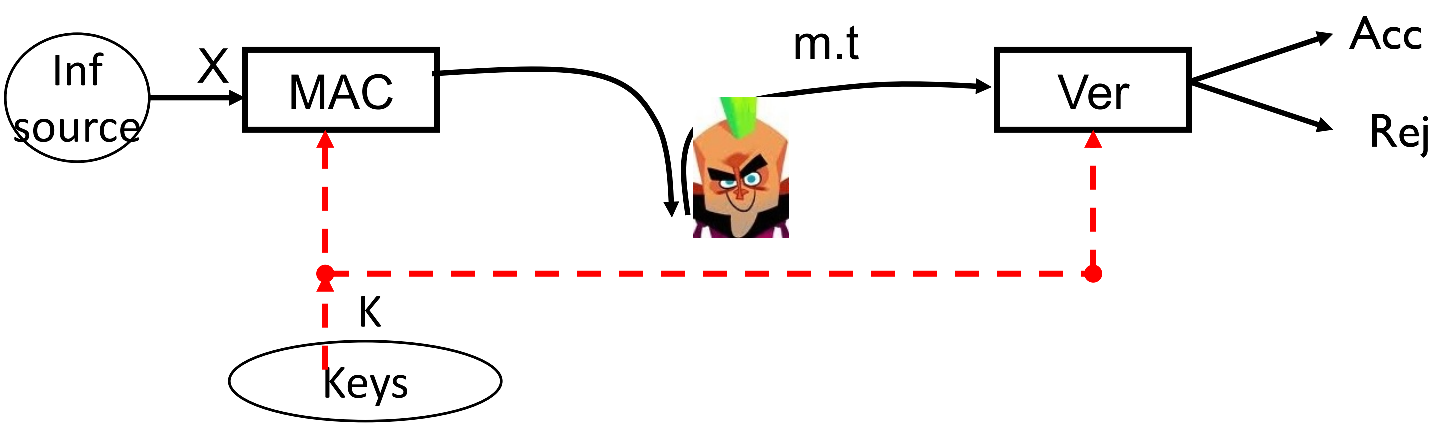
- Modeled as a game between

  (Alice & Bob)←→adversary

Model

- MAC system is public.
  - Set of messages, tags, keys and algorithms are public.

- Goal: constructing a forged message
  - (m,t) such that Ver ((m,t), k)=1
  - k is not known



Authentication games

- 0-message game
  - Impersonation game
  1. Adversary constructs a forgery
     - without seeing any communication.

- 1-message game
  - Substitution game
  1. Adversary sees an authenticated message
  2. Adversary constructs a forgery.

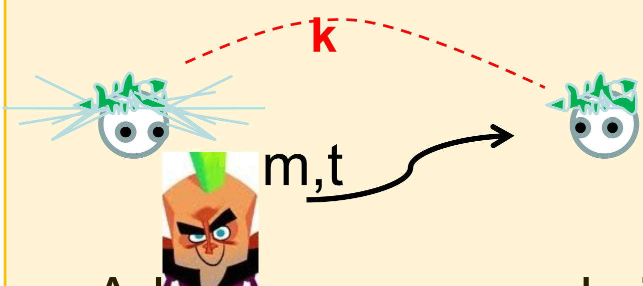
q-message game can be modelled based on above.

Authentication games

MAC system is Public

- Alice and Bob:
- Choose a secret random key k

- Adversary:
- Constructs m,t



- Adversary succeeds if:
- Ver ((m,t), k) =1

- 0-message game
  - Impersonation game
  1. Adversary constructs a forgery
     - without seeing any communication.

- P_0: Success probability in impersonation

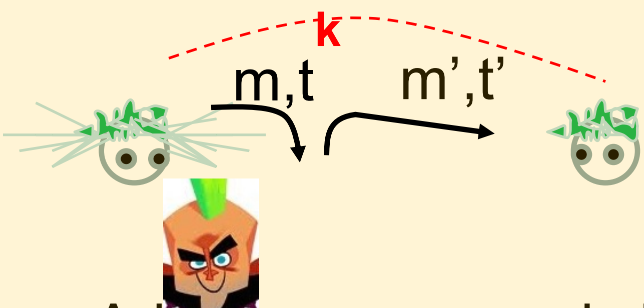
Authentication games

MAC system is Public

- Alice and Bob:
- Choose a secret random key k

- Adversary:

(i) sees m,t; (ii) constructs m',t'



- Adversary succeeds if:
- Ver ((m',t'), k) =1

- 1-message game
  – substitution game
  1. Adversary sees an authenticated message
  2. Adversary constructs a forgery.

- P_1: Success probability in substitution

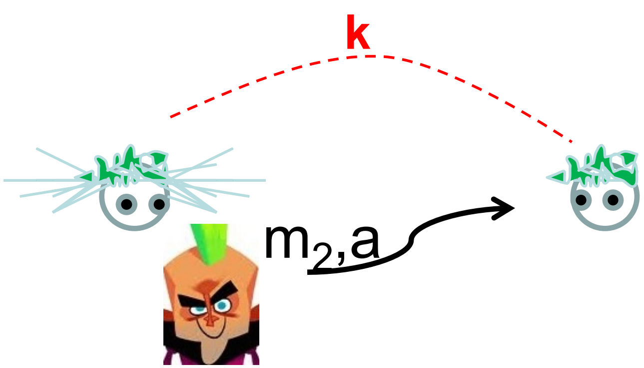
Example

- $M=\{m_1,m_2,m_3\}$, $K=\{k_1,k_2,k_3,k_4\}$, $T=\{a,b\}$
- Assume K is uniformly distributed.
- $P_0(m_2,a)$ = probability of success with (m_2,a)

= probability (m_2,a) be valid for the communicants' key

=1/2

	m_1	m_2	m_3
k_1	a	b	a
k_2	b	b	a
k_3	a	a	b
k_4	b	a	a



Two ways of writing
Encoding matrix

M

	m_1,b	m_1,a	m_2,b	m_2,a	m_3,b	m_3,a
k_1	0	1	1	0	0	1
k_2	1	0	1	0	0	1
k_3	0	1	0	1	1	0
k_4	1	0	0	1	0	1

0-message game

- $P_0(m,t)$ = Success probability with (m,t)
  = probability that (m,t) is valid for k

- Best success probability of attacker:

$$P_0 = \max_{m \in M,\, t \in T} P_0(m,t)$$

P_0 is success probability of impersonation game.

Example

- $M=\{m_1,m_2,m_3\}$, $K=\{k_1,k_2,k_3,k_4\}$, $T=\{a,b\}$
- Assume K is uniformly distributed.
- $P_0(m_2,a)$ = prob (m_2,a) is valid = 1/2
- $P_0(m_1,a) = 1/2$
- $P_0(m_3,a) = 3/4$
- …..
- $P_0 = \max_{\{(m_i, j) \in M \times T\}} P_0(m_i,j) = 3/4$

	m_1	m_2	m_3
k_1	a	b	a
k_2	b	b	a
k_3	a	a	b
k_4	b	a	a

Two ways of writing
Encoding matrix

M

	m_1,b	m_1,a	m_2,b	m_2,a	m_3,b	m_3,a
k_1	0	1	1	0	0	1
k_2	1	0	1	0	0	1
k_3	0	1	0	1	1	0
k_4	1	0	0	1	0	1

0-message game

- If the key distribution is not uniform:
  - Communicants' will choose a key according to probability distribution p(k)

- Probability (m,t) is valid:
  $P_0(m,t) = p\,(Ver((m,t), k)=1) = \Sigma_{\{k \in K,\ Ver((m,t),k)=1\}}\, p(k)$

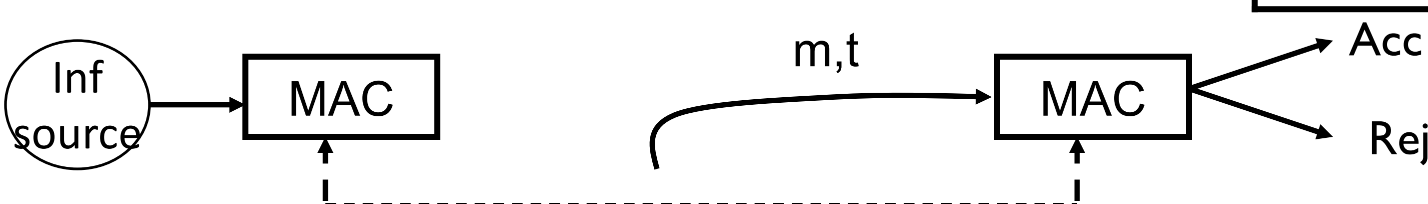
Possible adversary's choices

Communicant's choices		m_1,b	m_1,a	m_2,b	m_2,a	m_3,b	m_3,a
	k_1	0	1	1	0	0	1
	k_2	1	0	1	0	0	1
	k_3	0	1	0	1	1	0
	k_4	1	0	0	1	0	1

Success chance in 0-message

- $M=T=Z_3$, $K=Z_3 \times Z_3$,
- MAC $(m; (i,j)) = m.i + j \bmod 3$
- Assume $p(k)$ is uniform: $p(k) = 1/9$
- Adversary wants to choose *(m,t)* with highest $P_0(m,t)$
- Possible (m,t) pairs:
  {(0,0), (0,1), (0,2), (1,0), (1,1), (1,2), (2,0), (2,1), (2,2)}

K \ message	0	1	2
k1=(0,0)	0	0	0
k2=(0,1)	1	1	1
k3=(0,0)	2	2	2
k4=(1,0)	0	1	2
k5=(1,1)	1	2	0
k6=(1.2)	2	0	1
k7=(2,0)	0	2	1
k8=(2,1)	1	0	2
k9=(2,2)	2	1	0



Success chance

$P_0(0,0)$ = success prob with $(0,0)$

$= \Sigma_{\{k \in K,\ Ver((0,0),k)=1\}}\, p(k)$

$= 3 \times 1/9 = 1/3$

K \ message	0	1	2
k1	0	0	0
k2	1	1	1
k3	2	2	2
k4	0	1	2
k5	1	2	0
k6	2	0	1
k7	0	2	1
k8	1	0	2
k9	2	1	0

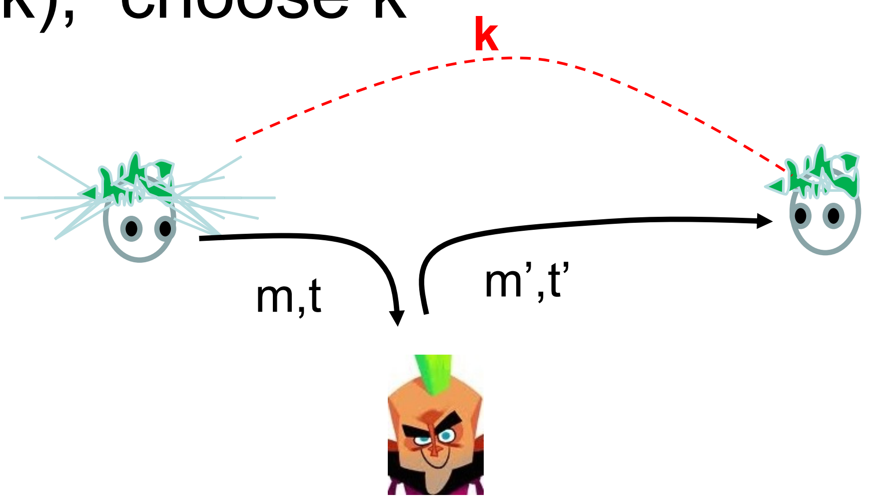
- $P_0(0,1)=3/9= 1/3$
- $P_0= \max_{\{m \in M,\ t \in T\}} P_0(m,t)$
- $P_0=1/3$

1-message game (substitution)

MAC system is public.

Alice and Bob:
- Choose distribution p(k), choose k

Alice:
- m ←p(m);
- t=MAC(m, k)



Adversary:
- Sees (m,t)
- forges m',t'

Adversary succeeds:
- Ver ((m',t'), k) =1, given Ver ((m,t), k) =1

Success chance: substitution game

- For each observed (m,t) pair:
- Adversary finds her best success cl
  - (m',t') that has the highest success cha
  - → (m',t') valid, given (m,t) is valid

	m_1	m_2	m_3
k_1	a	b	a
k_2	b	b	a
k_3	a	a	b
k_4	b	a	a

P((m',t'); (m,t)) is the success probability of forgery using (m',t') when (m,t) is seen.

Adversary's actions

	m_1,b	m_1,a	m_2,b	m_2,a	m_3,b	m_3,a
k_1	0	1	1	0	0	1
k_2	1	0	1	0	0	1
k_3	0	1	0	1	1	0
k_4	1	0	0	1	0	1

P((m_2,a); (m_1,a))=

$$\frac{p(k_3)}{p(k_3)+p(k_1)}$$

Success chance: substitution game

- $P((m_3,b)\ ;\ (m_1,a))= \dfrac{p(k_3)}{p(k_3)+p(k_1)} = \dfrac{1}{2}$
- $P((m_1,b)\ ;\ (m_{3,}\ a))= \dfrac{p(k_2)+p(k_4)}{p(k_1)+p(k_2)+p(k_4)} = \dfrac{2}{3}$

Adversary's actions

	m_1,b	m_1,a	m_2,b	m_2,a	m_3,b	m_3,a
k_1	0	1	1	0	0	1
k_2	1	0	1	0	0	1
k_3	0	1	0	1	1	0
k_4	1	0	0	1	0	1

Success chance of substitution

- Success chance of using (m’,t’) as forgery, when (m,t) is seen:

- P((m’,t’); (m,t))= p((m’,t’) valid | (m,t) valid)

$$= \frac{\sum_{k \in K \ s.t \ [(m',t')valid \ for \ k] \ AND \ [(m,t) \ valid \ for \ k]} p(k)}{\sum_{[(m,t) \ valid \ for \ k]} p(k)}$$

$$= \frac{\sum_{k \in K \ s.t.[Ver((m',t'),k)=1] \ AND \ [Ver((m,t),k)=1]} p(k)}{\sum_{[Ver((m,t),k)=1]} p(k)}$$

- Success chance of substitution when (m,t) is seen:

$$P_1(m,t) = \max_{\{m' \in M \;\; ,t' \in T\}} P(\,(m',t');\,(m,t))$$

- Success chance of substitution

$$P_1 = \max_{\{m \in M \;\; ,t \in T\}} P_1(m,t)$$

Success chance P_1

- Adversary sees (0,0) =(m,t)

- What (m',t') maximizes their success chance?

- Possible forgeries:

{(1,0), (1,1), (1,2), (2,0), (2,1), (2,2)}

- Which one?

key \ message	0	1	2
k1	0	0	0
k2	1	1	1
k3	2	2	2
k4	0	1	2
k5	1	2	0
k6	2	0	1
k7	0	2	1
k8	1	0	2
k9	2	1	0

Success chance P_1

- (0,0) is seen:
- P((1,0); (0,0))= success prob with (1,0), when (0,0) is seen

- P((1,0); (0,0))=

$$\frac{\Sigma_{\{k \in K,\ Ver((1,0),k)=1\ \&\ Ver((0,0),k)=1\}}\ p(k)}{\Sigma_{\{k \in K,\ Ver((0,0),k)=1)\}}\ p(k)}$$

$$= p(k)/\ [\Sigma_{\{k \in K,\ \ Ver((0,0),k)=1)\}}\ p(k)$$

$= (1/9)/(1/3)=1/3$

- P((1,1); (0,0)) =
- …….
- P((2,2); (0,0))
- $P_1(0,0) = \max_{\{m \in M,\ t \in T\}} P((m,t); (0,0)$

K \ message	0	1	2
k1	0	0	0
k2	1	1	1
k3	2	2	2
k4	0	1	2
k5	1	2	0
k6	2	0	1
k7	0	2	1
k8	1	0	2
k9	2	1	0

Impersonation or substitution?

- Adversary can play one of the two games: which game should they choose?

- P_0 must be compared with expected value of P_1.
  - For each message, expected success chance
    - (0,a),(0,b),(1,a),(1,b)(2,a),(2,b)
  - Averaged over all messages

→expected P1 can be smaller than P0

M / K	0	1	2
k_1	b	b	a
k_2	b	a	a
k_3	a	b	b
k_4	b	a	b

Gustavus Simmons
1930-

Bounds

- Brute force (generic) attacks give bounds on min success probability.

- Bounds

$$P \geq \frac{1}{|K|}$$

$$P_0 \geq \frac{1}{|T|}, \qquad P_1 \geq \frac{1}{|T|}$$

- An A-code is optimal if it satisfies one of the bounds.

S

Key \ message	0	1	2
k1	0	0	0
k2	1	1	1
k3	2	2	2
k4	0	1	2
k5	1	2	0
k6	2	0	1
k7	0	2	1
k8	1	0	2
k9	2	1	0

Example

- $M=T=Z_3$,
  MAC(m,k)= MAC(m, (a,b)= am+b
- $P_0 = P_1 = 1/3$
- Alice sends (m,t)=(1,2)
- 1a +b=2 ➔ b= 2 – a
- Suppose Alice sends a second message (0,0)

0.a+b=0 → b=0
→ a=2

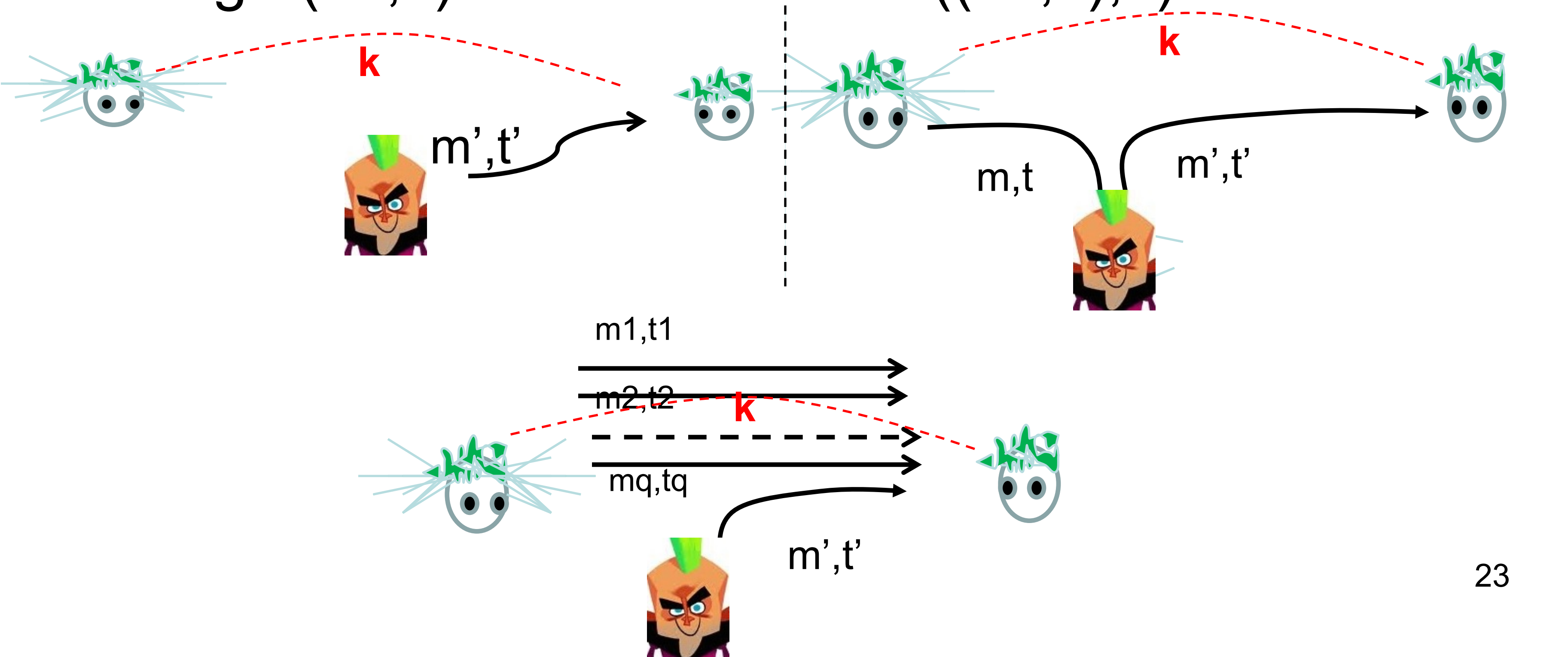
➔ Each key can be used once.
➔ Using the same key for two messages completely breaks the security.

Key (a, b) \ message	0	1	2
0,0	0	0	0
0,1	1	1	1
0,2	2	2	2
1,0	0	1	2
1,1	1	2	0
1,2	2	0	1
2,0	0	2	1
2,1	1	0	2
2,2	2	1	0

Security for q messages

- Adversary can see (choose) q message-tag pairs: (m_1,t_1), (m_2,t_2)…..$(m_q t_q)$- under same key

- Forge (m’,t’)   …such that Ver((m’,t’),k)=1



MAC applications

- The most widely used cryptographic primitive

- File integrity checking
  - Tampering with stored files

- Communication security
  - TLS data integrity
  - Secure file transfer

Summary

- Message integrity
  - Noise
  - Adversarial

- Protection goals:
  - Detection
  - Correction

Adversarial corruption

- A-codes
  - MAC, Ver, success prob

- 0-message security
  - Impersonation
- 1-message security
  - Substitution
- q-message security
  - Wegman-Carter

- Bounds