Politecnico di Torino

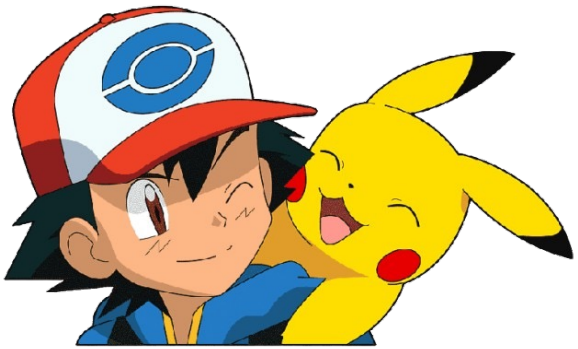
Gotta prove 'em all!

come funzionano definizioni (e dimostrazioni) di sicurezza in crittografia

Lorenzo Romano

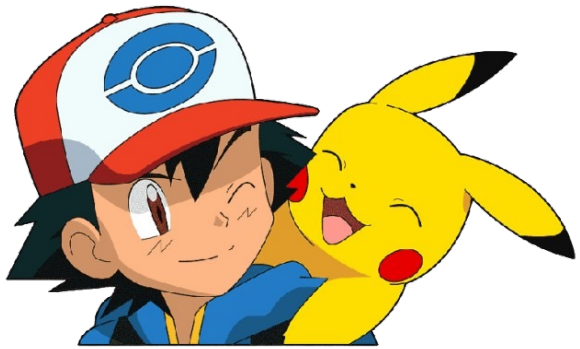
CrypTO
Crittografia e Teoria dei Numeri

Obiettivi di questo talk



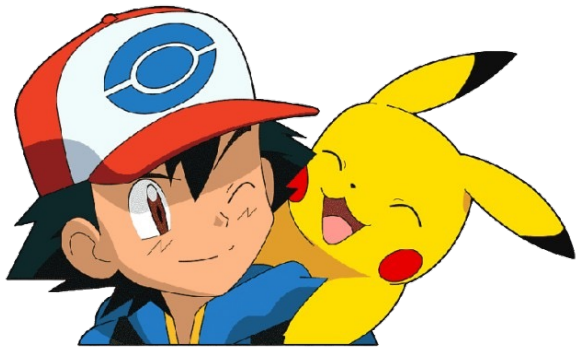
Obiettivi di questo talk

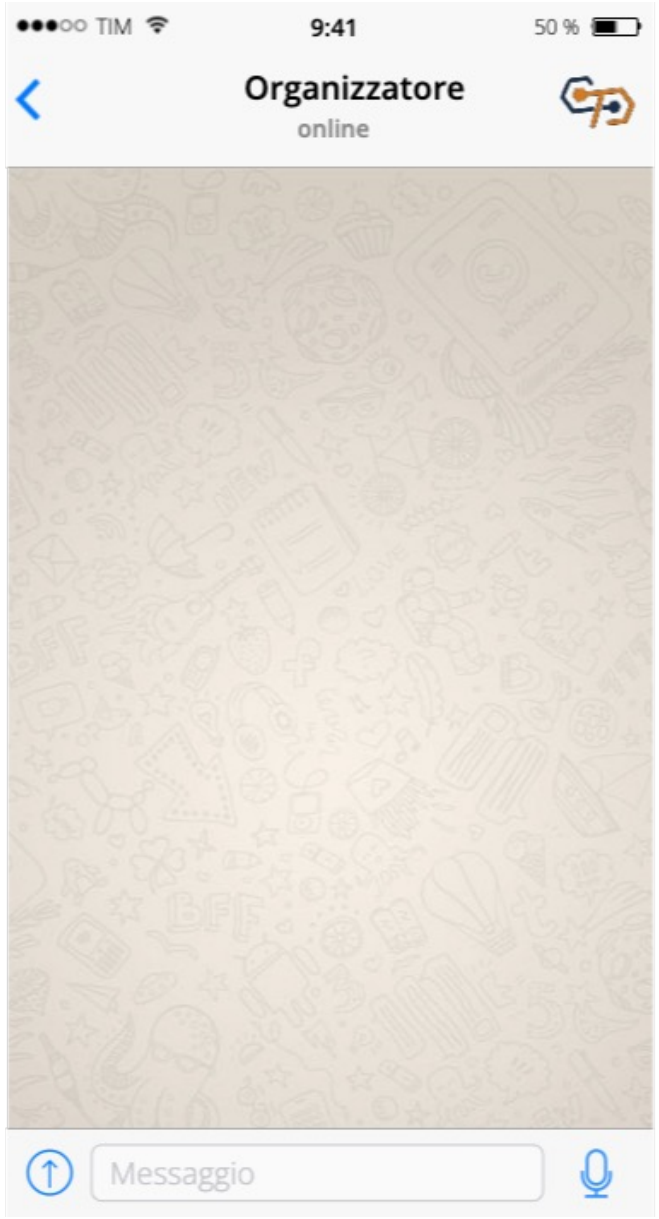
- La Crittografia è matematica anche nel metodo

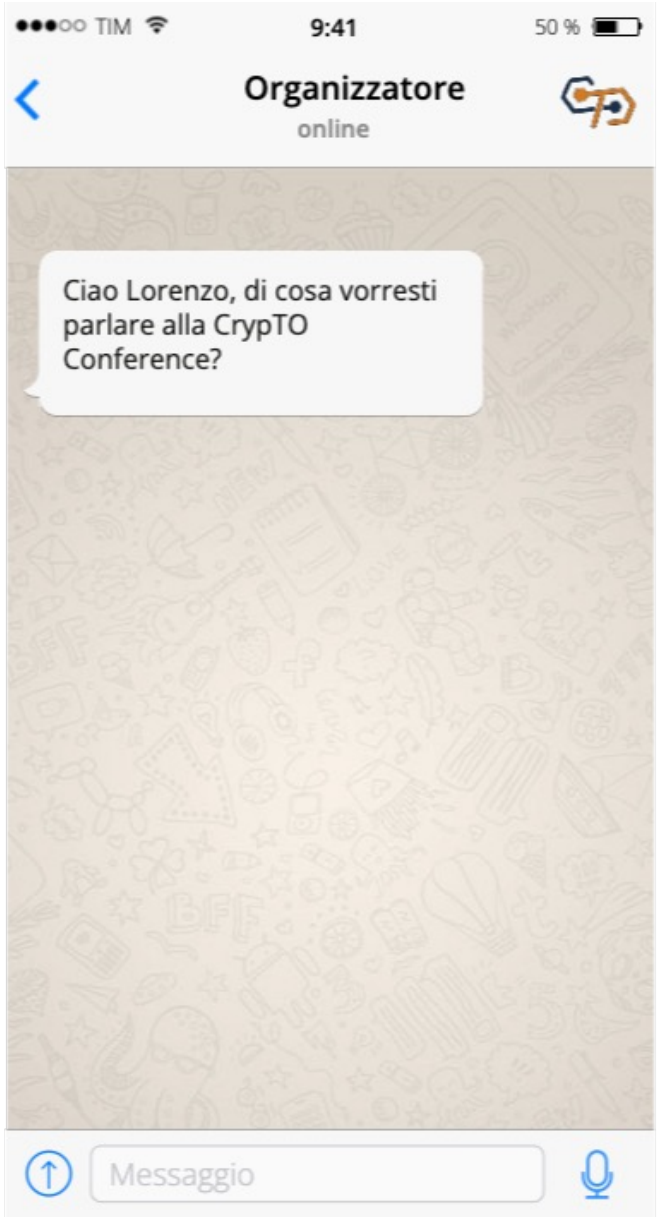


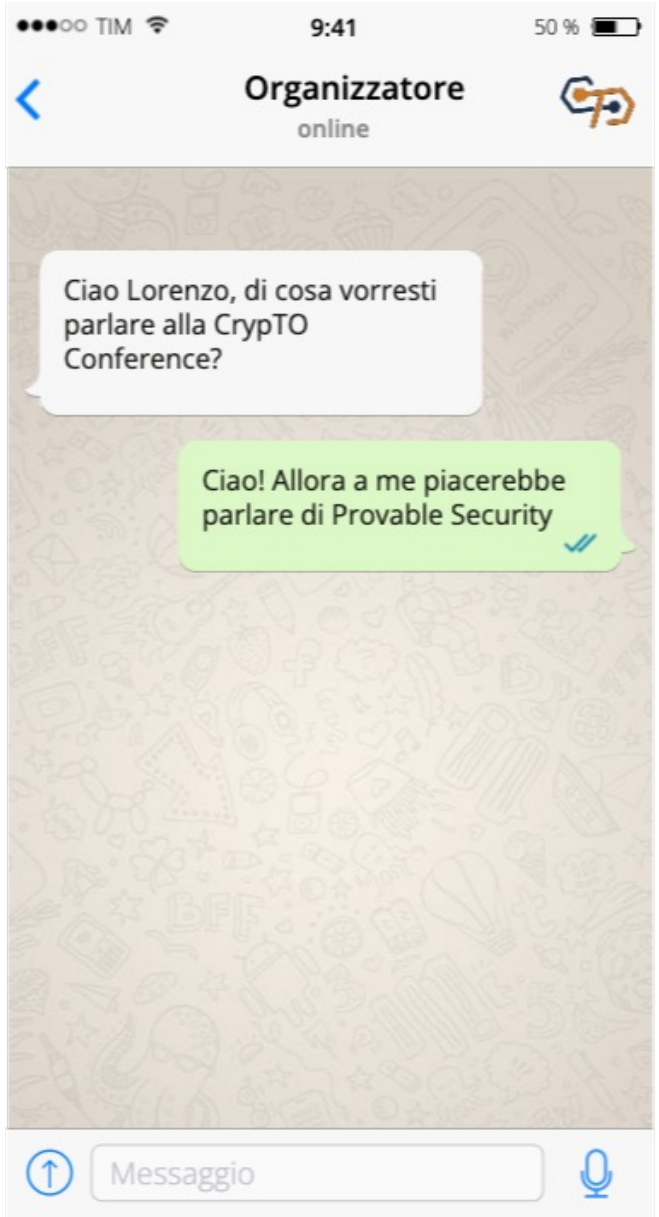
Obiettivi di questo talk

- La Crittografia è matematica anche nel metodo
- Cosa significa che un protocollo è **sicuro**?




TIM
9:41
50 %
Organizzatore
online
Messaggio


●●●○○ TIM
9:41
50 %
Organizzatore
online
Ciao Lorenzo, di cosa vorresti parlare alla CrypTO Conference?
Messaggio


TIM
9:41
50 %
Organizzatore
online
Ciao Lorenzo, di cosa vorresti parlare alla CrypTO Conference?
Ciao! Allora a me piacerebbe parlare di Provable Security
Messaggio


TIM
9:41
50 %
Organizzatore
online
Ciao Lorenzo, di cosa vorresti parlare alla CrypTO Conference?
Ciao! Allora a me piacerebbe parlare di Provable Security
Mmm, non è un argomento un po' troppo tecnico?
Messaggio


●●●○○ TIM
9:41
50 %
Organizzatore
online
Ciao Lorenzo, di cosa vorresti parlare alla CrypTO Conference?
Ciao! Allora a me piacerebbe parlare di Provable Security
Mmm, non è un argomento un po' troppo tecnico?
Potrebbe sembrarlo, ma in realtà è uno dei punti chiave in cui si distinguono crittografia classica e moderna
Messaggio


TIM
9:41
50 %
Organizzatore
online
Ciao Lorenzo, di cosa vorresti parlare alla CrypTO Conference?
Ciao! Allora a me piacerebbe parlare di Provable Security
Mmm, non è un argomento un po' troppo tecnico?
Potrebbe sembrarlo, ma in realtà è uno dei punti chiave in cui si distinguono crittografia classica e moderna
Messaggio


●●●○○ TIM
9:41
50 %
Organizzatore
online
Ciao! Allora a me piacerebbe parlare di Provable Security
Mmm, non è un argomento un po' troppo tecnico?
Potrebbe sembrarlo, ma in realtà è uno dei punti chiave in cui si distinguono crittografia classica e moderna
Comunque farei solo un'introduzione
Messaggio


●●●○○ TIM
9:41
50 %
Organizzatore
online
Mmm, non è un argomento un po' troppo tecnico?
Potrebbe sembrarlo, ma in realtà è uno dei punti chiave in cui si distinguono crittografia classica e moderna
Comunque farei solo un'introduzione
Ok, ma che sia divulgativa. Fatti venire in mente una qualche idea
Messaggio


my linkedin profile
R, python, javascript, shiny, dplyr, purrr, ditto,
ggplot, d3, canvas, spark, sawk, pyspark, sparklyR,
lodash, lazy, bootstrap, jupyter, vulpix, git,
flask, numpy, pandas, feebas, scikit, pgm, bayes,
h2o.ai, sparkling-water, tensorflow, keras, onyx,
ekans, hadoop, scala, unity, metapod, gc, c#/c++,
krebase, neo4j, hadoop.
I typically ask recruiters to point out which of these are pokemon.


Pokémon™
Blue Version
©'95.'96.'98 GAME FREAK inc.

Lo scenario

Lo scenario

Lo scenario

Lo scenario

Lo scenario

Schemi di cifratura

Schemi di cifratura

- Ogni protocollo ha un suo obiettivo (goal) di sicurezza

Schemi di cifratura

- Ogni protocollo ha un suo obiettivo (goal) di sicurezza
- Confidenzialità (privacy)

Schemi di cifratura

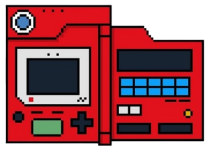
- Ogni protocollo ha un suo obiettivo (goal) di sicurezza
- Confidenzialità (privacy)
- Cos'è? Come si raggiunge?

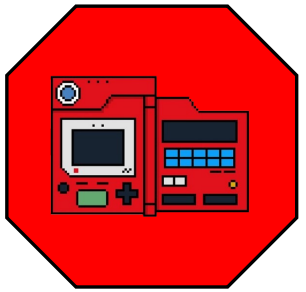
Schemi di cifratura

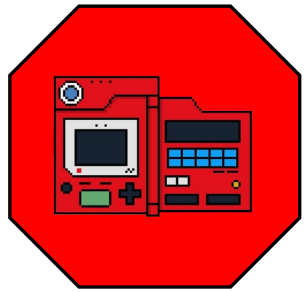
- Ogni protocollo ha un suo obiettivo (goal) di sicurezza
- Confidenzialità (privacy)
- Cos'è? Come si raggiunge?

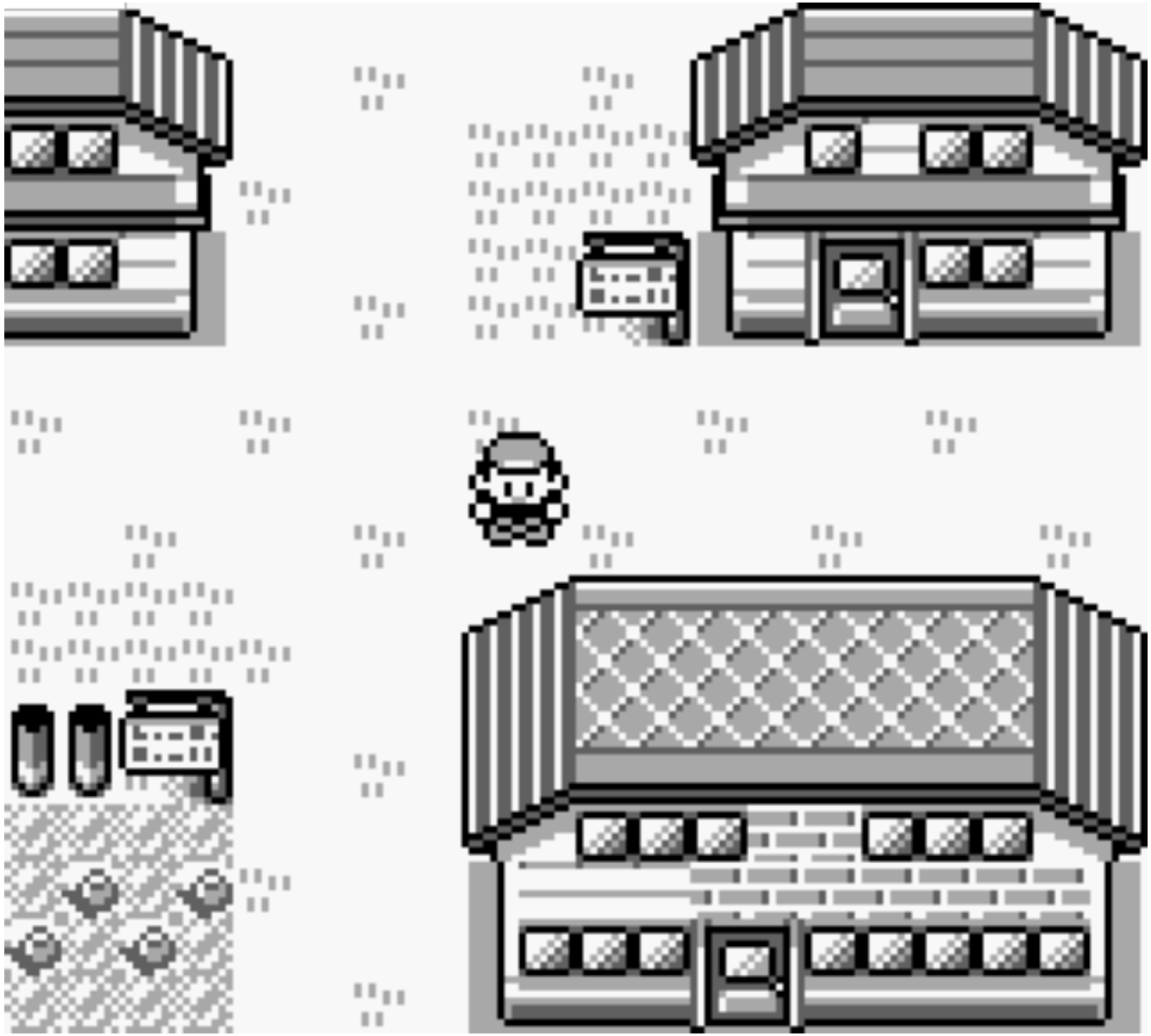
Definizioni di sicurezza:

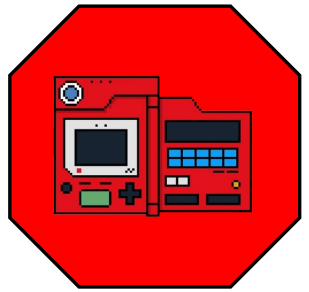
catturano proprietà fondamentali degli obiettivi di sicurezza di un protocollo crittografico e le quantificano

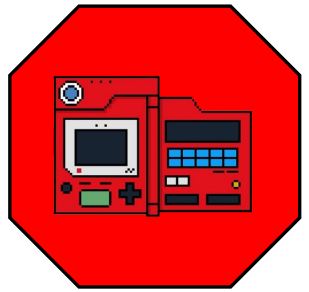




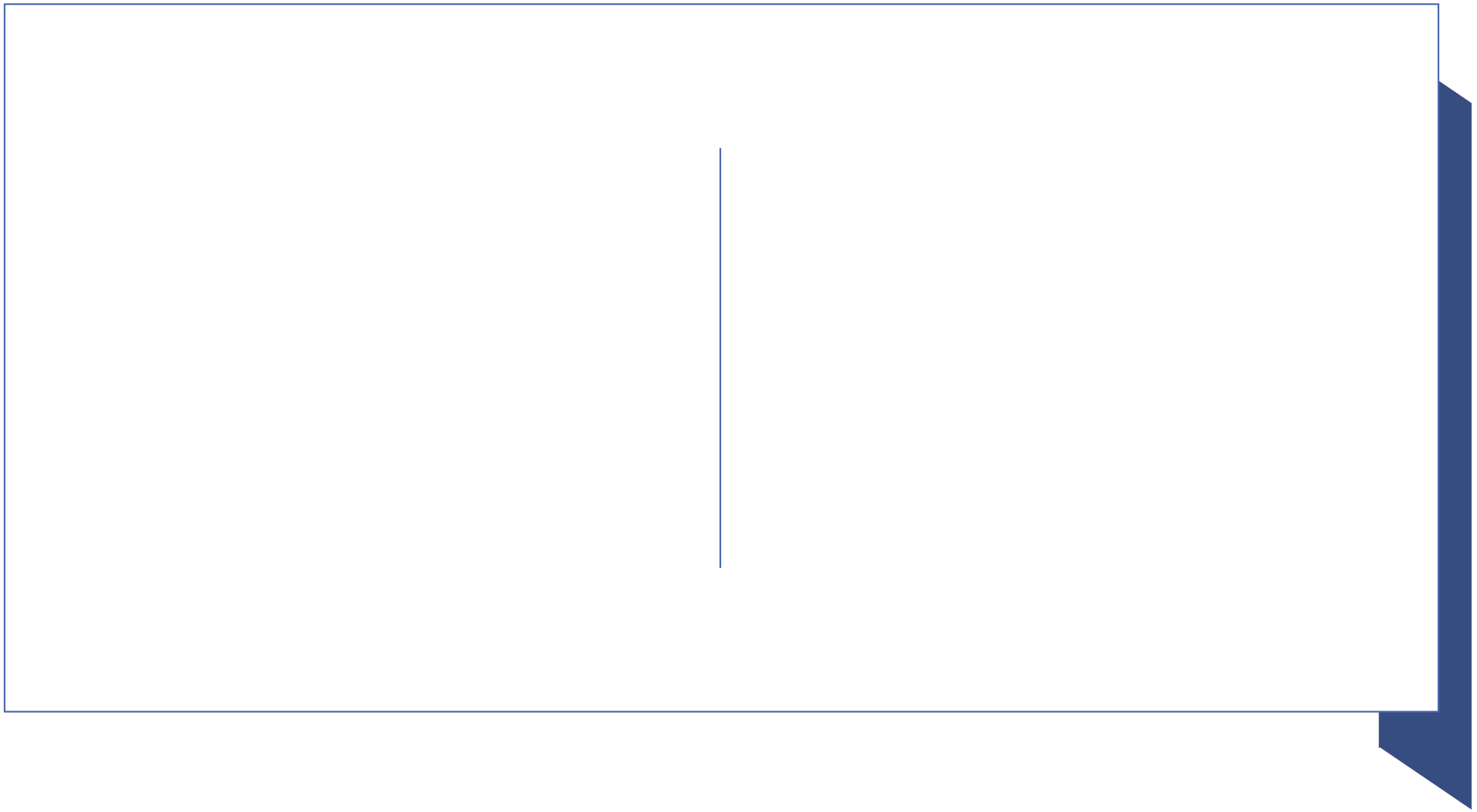









Wild MISSINGNO.
appeared!




Wild MEW
appeared!

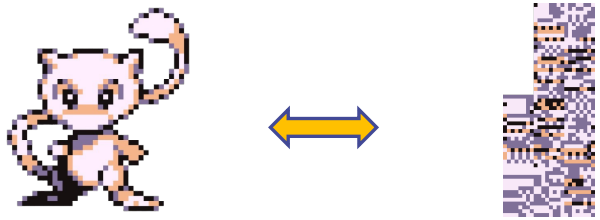

Wild MEW
appeared!


Wild MISSINGNO.
appeared!


▶BALL×30
BAIT
THROW ROCK
RUN

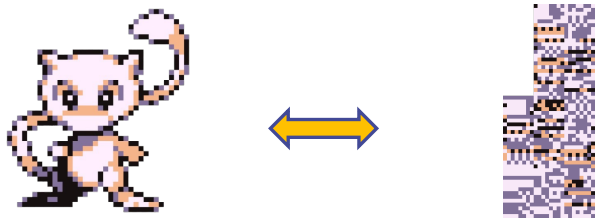
(una slide seria)

(una slide seria)



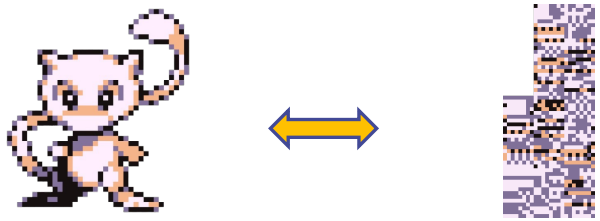
(una slide seria)

- Ash vince se indovina la natura di MissingNo



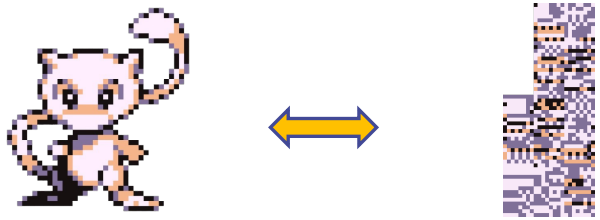
(una slide seria)

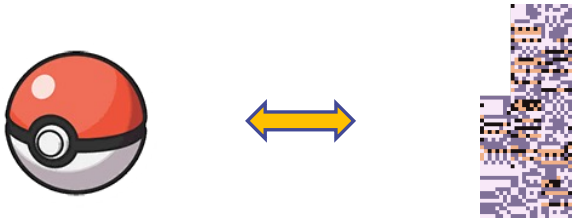
- Ash vince se indovina la natura di MissingNo
- La sua probabilità di vittoria è sempre $\geq \frac{1}{2}$



(una slide seria)

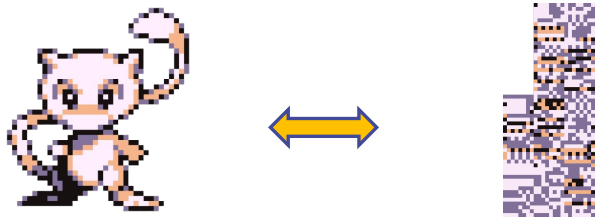
- Ash vince se indovina la natura di MissingNo
- La sua probabilità di vittoria è sempre $\geq \frac{1}{2}$



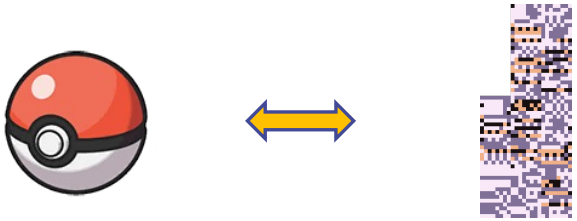


(una slide seria)

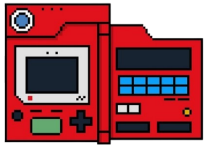
- Ash vince se indovina la natura di MissingNo
- La sua probabilità di vittoria è sempre $\geq \frac{1}{2}$



- Sicurezza di uno schema: Ash può solo tirare a caso

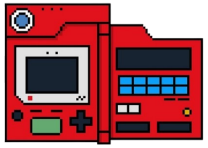


Glossario



Glossario

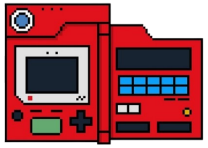
Chiave



Glossario

Chiave

Avversario

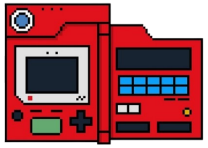


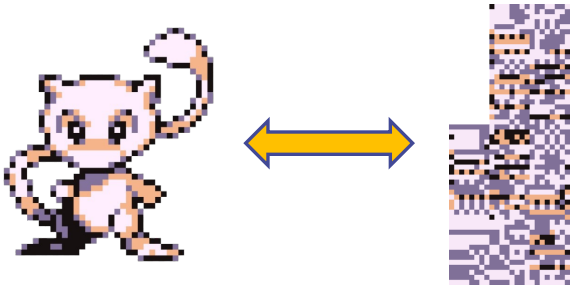
Glossario

Chiave

Avversario

Oracolo





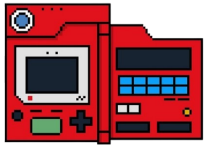
Glossario

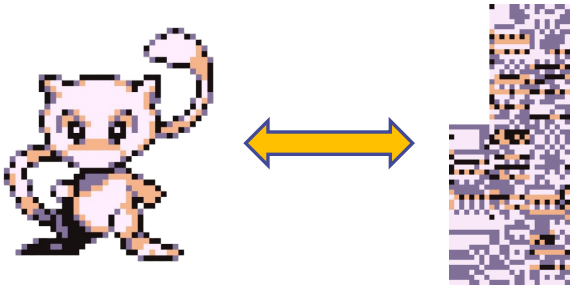
Chiave

Avversario

Oracolo

Gioco/esperimento





Glossario

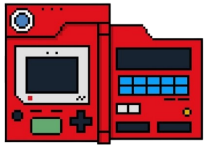
Chiave

Avversario

Oracolo

Gioco/esperimento

Vantaggio



Glossario

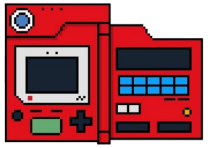
Chiave

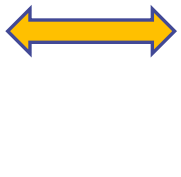
Avversario

Oracolo

Gioco/esperimento

Vantaggio





Glossario

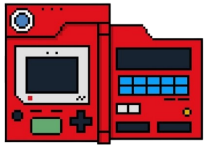
Chiave

Avversario

Oracolo

Gioco/esperimento

Vantaggio



Glossario

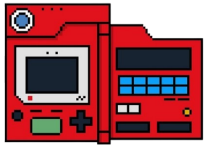
Chiave

Avversario

Oracolo

Gioco/esperimento

Vantaggio



Glossario

Indistinguibilità

Conclusione

Conclusione

- Ogni protocollo ha un suo obiettivo di sicurezza

Conclusione

- Ogni protocollo ha un suo obiettivo di sicurezza
- Ogni obiettivo ha una sua nozione corrispondente

Conclusione

- Ogni protocollo ha un suo obiettivo di sicurezza
- Ogni obiettivo ha una sua nozione corrispondente
- Ciascuna nozione si definisce attraverso un gioco

Conclusione

- Ogni protocollo ha un suo obiettivo di sicurezza
- Ogni obiettivo ha una sua nozione corrispondente
- Ciascuna nozione si definisce attraverso un gioco
- Possono esistere diverse nozioni per uno stesso obiettivo

Cosa fa la Provable Security

Cosa fa la Provable Security

- **Definisce** nozioni di sicurezza per un obiettivo

Cosa fa la Provable Security

- **Definisce** nozioni di sicurezza per un obiettivo
- Mette in relazione diverse nozioni

Cosa fa la Provable Security

- **Definisce** nozioni di sicurezza per un obiettivo
- Mette in relazione diverse nozioni
- Verifica che un protocollo soddisfi una data nozione di sicurezza attraverso **dimostrazioni**

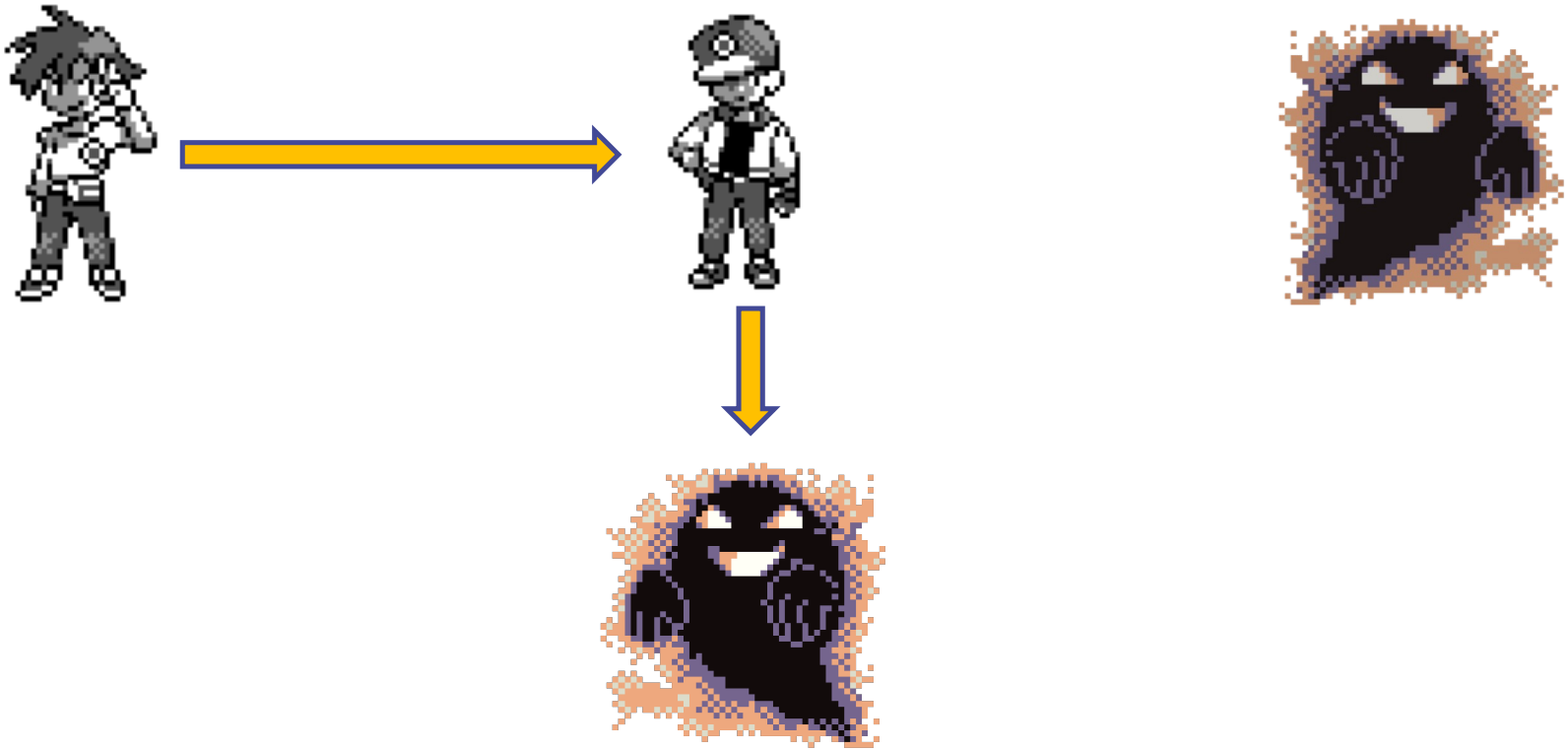
Riduzioni

(Riduzioni)

Riduzioni

(Riduzioni)

Riduzioni



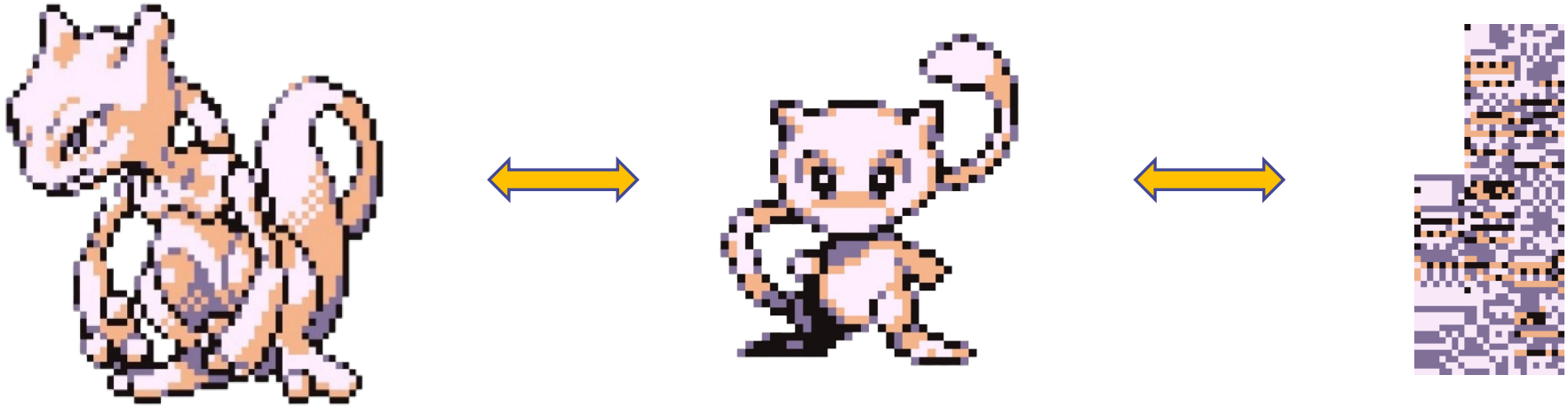
(Sequenze di giochi)

(Sequenze di giochi)

(Sequenze di giochi)

(Sequenze di giochi)

(Sequenze di giochi)



Gotta prove 'em all!

The End

Politecnico
di Torino

CrypTO
Crittografia e Teoria dei Numeri

The End

Politecnico di Torino

1859

CrypTO

Crittografia e Teoria dei Numeri

The End

Grazie per l'attenzione!

Politecnico di Torino

CrypTO
Crittografia e Teoria dei Numeri