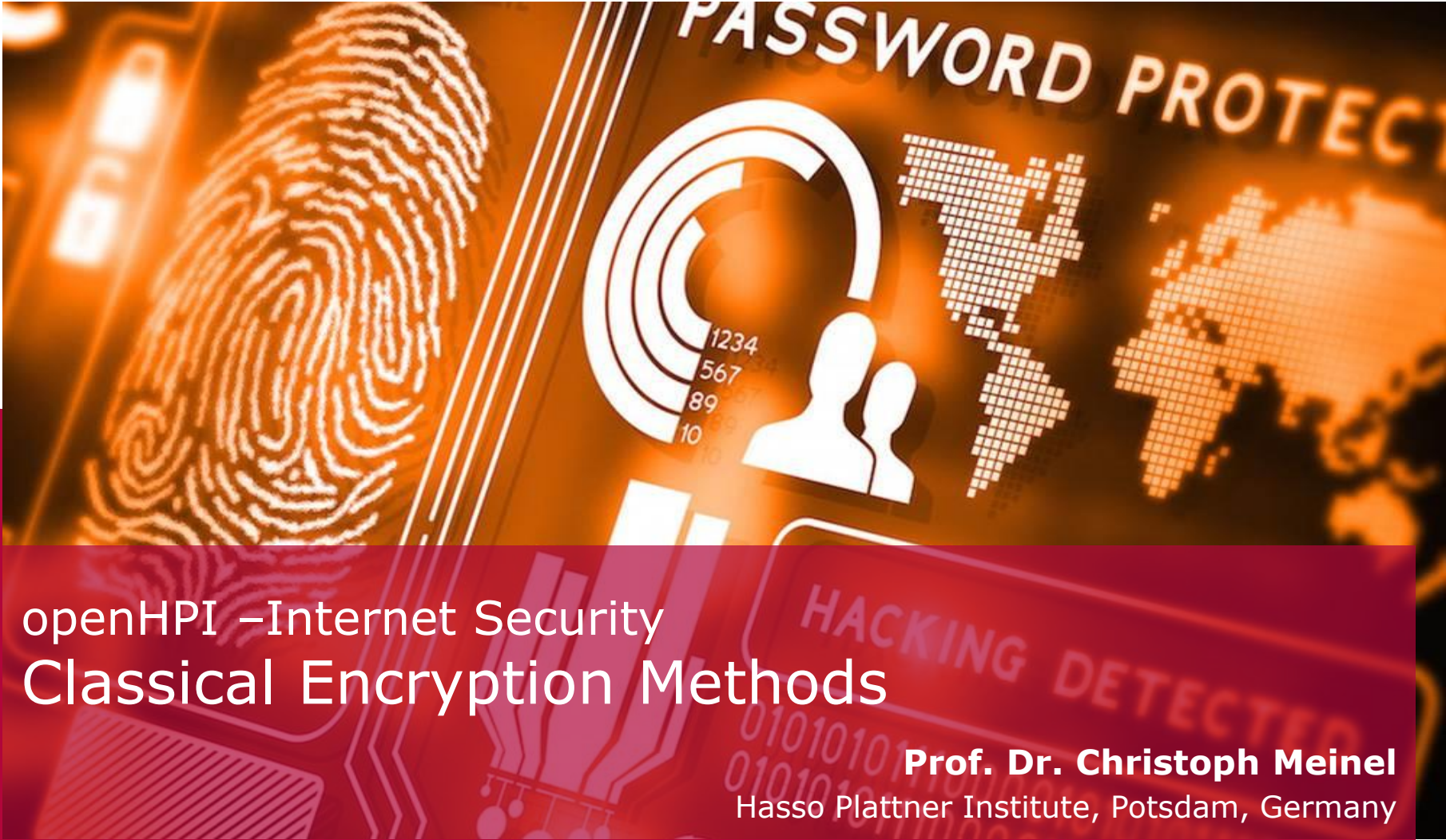




openHPI – Internet Security Classical Encryption Methods

Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Potsdam, Germany

Encryption with Monoalphabetic Substitution (1/2)

In encryption by **monoalphabetic substitution**, plaintext is substituted - **encrypted** - with a cipher text using the same alphabet as the plaintext

- Substitution schemes for encryption can be chosen arbitrarily but must be disclosed to all communication subscribers, e.g.
 - Switching the alphabetic sequence ($A \Leftrightarrow Z, B \Leftrightarrow Y, \dots$)
 - Shifting the alphabet to a specific position
 - Encryption with start word
 - ...

Encryption with start word

- Participant select start word
- Alphabet is appended to the start word
- Then all multiple occurrences of characters are deleted
- **Example:**
 - Participants select start word "INTERNETSECURITY", then
 - Add the alphabet to INTERNETSECURITY and delete all repeat occurrences of letters: "INTERSCUY" followed by the remaining letters of the alphabet



Encryption with Substitution Cipher (1/2)

Substitution cipher, in which each letter is replaced by the letter following the X position (encryption key) in the alphabet

Example:

- Sender and receiver select (latin) alphabet and agree on key (shift number) $X = 12$

□ Plaintext: „INTERNET SECURITY“

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---



Encrypt with $X = 12$



Decrypt with $X = -12$

M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

- Encrypted text: „UZFQDZQF EQOGDUFK“
- **Note:** If X is a multiple of the size of the alphabet, then encrypted text = plaintext

Encryption with Substitution Cipher (2/2)

Required for cracking the key X:

- If it is known that it is a replacement cipher, an attacker needs a maximum of $\#\{\text{alphabet}\}$ attempts, in our example, a maximum of 26 attempts
 - An attacker then replaces all the letters with the letters following $X = 1$ positions, then 2, 3, 4, and so on, and checks each time whether the result produces a meaningful text
- **Caesar cipher:**
 - A special case of substitution cipher with $X = 3$, where "A" is translated into a "D" ...

Encryption with Polyalphabetic Ciphers

With **polyalphabetic ciphers**, several "secret" alphabets are used

- The same characters in the plaintext can thus be converted into different letters in the secret text and vice versa
- **Example:**
 - The number of "shifts" is selected for each character depending on the position in the word, e.g.
 - Position determines shift: e.g. "INTERNET"
 - "I" at position 1 is shifted by 1 → "I" is replaced by "J"
 - "N" at position 2 is shifted by 2 → "N" is replaced by "P"
 - "T" at position 8 is shifted by 8 → "T" is replaced by "B"
 - „INTERNET “ → „JPWIIWTLB “

Encryption with Vigenère Encryption (1/2)

- ... developed by Blaise de Vigenère in the 16th century
- Choice of a keyword, e.g. "SECURE" (in the following the positions of the letters in the alphabet are used: A = 0, B = 1, C = 2, ...)
- Each letter in the plaintext is shifted according to the position of the corresponding keyword letter in the alphabet

Plaintext	I	N	T	E	R	N	E	T
Cipher text	S	E	C	U	R	E	S	E
Shifts	18	4	2	20	17	4	18	4
Cipher	A	R	V	Y	I	R	W	X

- If the length of the text is not a multiple of the key length, this is truncated at the end ...

Vigenère cipher can be cracked:

- If text is long enough, attackers can determine key length(s):
Each n^{th} character is encoded with the same replacement code, which can be decoded by frequency analysis ...

Vigenère variant with autokey:

- Cipher text consists of **cipher word** followed by **plaintext**

Plaintext	I	N	T	E	R	N	E	T	S	E	C	U	R	I	T	Y
Cipher text	S	E	C	U	R	E	I	N	T	E	R	N	E	T	S	E
Cipher	A	R	V	Y	I	R	M	G	L	I	T	H	V	B	L	C

- Receiver can decrypt the first characters with keyword and the following characters can be decoded with already decrypted text

Decryption by Cryptoanalysis (1/2)

Cryptoanalysis - how can encryption be cracked?

Kerckhoff's principle:

- The security of an encryption process should be based **solely** on the secrecy of the key and **not** on the confidentiality of the procedure

Kerckhoff recommends publicizing encryption procedures in order to enable many experts to analyze and to identify possible weaknesses as quickly as possible

Decryption by Cryptoanalysis (2/2)

Attack opportunities:

■ Brute Force:

- Systematic attempts with all possible keys

■ Dictionary attacks:

- Systematic attempts with frequently used or familiar keywords

■ Statistical analyses:

- Possible on the basis of linguistic observations, e.g. amount of letters in words of a language

■ Chosen plaintext:

- Analysis of the encryption of a known text